QLOGIC

Simplify

SANbox2-8c Fibre Channel Switch

Installation Guide

Firmware Version 5.0

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

This SANbox switch is covered by one or more of the following patents: 6697359; other patents pending.

Document Revision History

Release, Revision A, February 2005	Firmware Version 5.0 SANsurfer Switch Manager Version 5.00

Table of Contents

Section 2 General Description

Section 3 Planning

Section 5 Diagnostics/Troubleshooting

Appendix A Specifications

Appendix B Command Line Interface

Figures

Tables

Notes

Section 1

Introduction

This manual describes the features and installation of the SANbox2-8c Fibre Channel switch, firmware version 5.0. This manual is organized as follows:

- Section 1 describes the intended audience, related materials, safety notices, communications statements, laser safety information, electrostatic discharge sensitivity precautions, accessible parts, general program license, and technical support.
- Section 2 is an overview of the switch. It describes indicator LEDs and all user controls and connections.
- Section 3 describes the factors to consider when planning a fabric.
- Section 4 explains how to install and configure the switch.
- Section 5 describes the diagnostic methods and troubleshooting procedures.
- Appendix A lists the switch specifications.
- Appendix B describes the Command Line Interface.

Please read the communications statements and laser safety information later in this section. Use this manual with the *SANbox2-8c/16 Switch Management User's Guide*.

1.1 Intended Audience

This manual introduces users to the switch and explains its installation and service. It is intended for users who are responsible for installing and servicing network equipment.

1.2 Related Materials

The following manuals and materials are referenced in the text and/or provide additional information.

- *SANbox2-8c/16 Switch Management User's Guide*, publication number 59022-11.
- *QLogic Switch Interoperability Guide v3.0*. This PDF document can be downloaded at http://www.qlogic.com/interopguide/info.asp#inter.
- RFC 2865 *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2869 *RADIUS Extensions*
- Fibre Channel-Arbitrated Loop (FC-AL-2) Rev. 6.8.
- Fibre Channel-10-bit Interface Rev. 2.3.
- Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard (draft-ietf-ipfc-fabric-element-mib-04.txt).

The Fibre Channel Standards are available from:

Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5776 Phone: (800) 854-7179 or (303) 397-7956
Fax: (303) 397-2740.

1.3
New in this Release

The following items are new in the current firmware release:

- Support for FC-SP device security for authorization and authentication.
- Support for centralized device and user authentication on a Remote Authentication Dial-In User Service (RADIUS) server.
- Support for secure workstation connections to the switch using the Secure Shell (SSH) protocol for the Telnet command line interface and the Secure Socket Layer protocol for management applications such as SANsurfer Switch Manager.
- Support for transmission of service indications to Common Information Module (CIM) clients through the configuration of listeners and subscriptions.
- Support for centralized control of switch services: Telnet, Secure Shell (SSH) connections, SANsurfer Switch Manager, Secure Socket Layer (SSL) connections, Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), File Transfer Protocol (FTP), Common Information Module (CIM), and management server.
- Centralized control of switch services: Telnet, SANsurfer Switch Manager, Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), File Transfer Protocol (FTP), Common Information Module (CIM), and management server.
- Maximum number of zones is increased to 2000.
- Time zone can be set to synchronize the switch and workstation.
- Support for SANsurfer Switch Manager on MacIntosh and S.u.S.E Linux operating systems.

1.4 Safety Notices

A **Warning** notice indicates the presence of a hazard that has the potential of causing personal injury.

4-3, 4-17

A **Caution** notice indicates the presence of a hazard that has the potential of causing damage to the equipment.

4-4, 5-14

1.5 Sicherheitshinweise

Ein **Warnhinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Verletzungen zur Folge hat.

4-3, 4-18

Ein **Vorsichtshinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Geräteschäden zur Folge hat.

4-4, 5-14

1.6 Notes informatives relatives à la sécurité

Une note informative **Avertissement** indique la présence d'un risque pouvant entraîner des blessures.

4-3, 4-17

Une note informative **Attention** indique la présence d'un risque pouvant entraîner des dégâts matériels.

4-4, 5-14

1.7 Communications Statements

The following statements apply to this product. The statements for other products intended for use with this product appear in their accompanying manuals.

1.7.1 Federal Communications Commission (FCC) Class A Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause unacceptable interference, in which case the user will be required to correct the interference at their own expense.

Neither the provider nor the manufacturer is responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

1.7.2 Canadian Department of Communications Class A Compliance Statement

This equipment does not exceed Class A limits for radio emissions for digital apparatus, set out in Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

1.7.3
Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques por les appareils numériques, telles que prescrites par le Réglement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécwssaires pour en éliminer les causes.

1.7.4
CE Statement

The CE symbol on the equipment indicates that this system complies with the EMC (Electromagnetic Compatibility) directive of the European Community (89/336/EEC) and to the Low Voltage (Safety) Directive (73/23/EEC). Such marking indicates that this system meets or exceeds the following technical standards:

- EN60950/A11:1997 – “Safety of Information Technology Equipment, Including Electrical Business Equipment”.
- EN55022:1998 – “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment”.
- EN55024-1:1998 – “Electromagnetic compatibility - Generic immunity standard Part 1: Residential commercial, and light industry.”
  - IEC1000-4-2:1995 – “Electrostatic Discharge Immunity Test”
  - IEC1000-4-3:1995 – “Radiated, Radio-Frequency, Electromagnetic Field Immunity Test”
  - IEC1000-4-4:1995 – “Electrical Fast Transient/Burst Immunity Test”
  - IEC1000-4-5:1995 – “Surge Immunity Test”
  - IEC1000-4-6:1996 – “Immunity To Conducted Disturbances, Induced By Radio-Frequency Fields”
  - IEC1000-4-8:1993 – "Power Frequency Magnetic Field Immunity Test”
  - IEC1000-4-11:1994 – “Voltage Dips, Short Interruptions And Voltage Variations Immunity Tests”
- EN61000-3-2:1995 – “Limits For Harmonic Current Emissions (Equipment Input Current Less Than/Equal To 16 A Per Phase)” Class A
- EN61000-3-3:1995 – “Limitation Of Voltage Fluctuations And Flicker In Low-Voltage Supply Systems For Equipment With Rated Current Less Than Or Equal To 16 A”

1.7.5
VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

1.7.6
BSMI Class A Statement

警告使用者:

這是甲類的資訊產品, 在居住的環境中使用時, 可能會造成射頻干擾, 在這種情況下, 使用者會被要求採取某些適當的對策.

Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

1.8 Laser Safety Information

This product may use Class 1 laser optical transceivers to communicate over the fiber optic conductors. The U.S. Department of Health and Human Services (DHHS) does not consider Class 1 lasers to be hazardous. The International Electrotechnical Commission (IEC) 825 Laser Safety Standard requires labeling in English, German, Finnish, and French stating that the product uses Class 1 lasers. Because it is impractical to label the transceivers, the following label is provided in this manual.

1.9 Electrostatic Discharge Sensitivity (ESDS) Precautions

The assemblies used in the switch chassis are ESD sensitive. Observe ESD handling procedures when handling any assembly used in the switch chassis.

1.10 Accessible Parts

The Field Replaceable Units (FRUs) in the SANbox2-8c switch are the following:

- Small Form-Factor Pluggable (SFP) optical transceivers

1.11 Pièces Accessibles

Les pièces remplaçables, Field Replaceable Units (FRU), du commutateur SANbox2-8c Fibre Channel Switch sont les suivantes:

- Interfaces aux media d’interconnexion appelés SFP transceivers.

1.12 Zugängliche Teile

Nur die folgenden Teile im SANbox2-8c Fibre Channel Switch können kundenseitig ersetzt werden:

- Schnittstellen für die Zwischenverbindungsträger, SFP transceivers genannt.

1.13 General Public License

QLogic® Fibre Channel switches are powered by the Linux® operating system. A machine-readable copy of the Linux source code is available upon written request to the following address. A nominal fee will be charged for reproduction, shipping, and handling costs in accordance with the General Public License.

QLogic Corporation
6321 Bury Drive
Eden Prairie, MN 55346-1739
Attention: Technical Support - Source Request

Warning: Installation of software or files not authorized by QLogic will immediately and irrevocably void all warranty and service contracts on the affected units.

The following general public license has been reproduced with permission from:

GNU General Public License
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

1.13.1 Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

1.13.2
Terms And Conditions For Copying, Distribution And Modification

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such

modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the

rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

11. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this

License, you may choose any version ever published by the Free Software Foundation.

12. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

13. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

14. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

1.13.3 How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) *yyyy name of author*

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) *year name of author*

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

> *signature of Ty Coon*, 1 April 1989
> Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

1.14 Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

1.14.1 Availability

QLogic Technical Support is available from 7:00 AM to 7:00 PM Central Standard Time, Monday through Friday, excluding QLogic-observed holidays.

1.14.2 Training

QLogic offers certification training for the technical professional for both the SANblade™ HBAs and the SANbox2™ switches. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com.

1.14.3 Contact Information

Telephone:	+1 952-932-4040
Fax:	+1 952-932-4018
Email:	
Technical Service	support@qlogic.com
Technical Training	tech.training@qlogic.com
Support Web Site:	support.qlogic.com

Section 2

General Description

This section describes the features and capabilities of the SANbox2-8c Fibre Channel switch. The following topics are described:

- Chassis Controls and LEDs
- Fibre Channel Ports
- Ethernet Port
- Serial Port
- Power Supply and Fan
- Switch Management

Fabrics are managed with the SANsurfer Switch Manager™ switch management application (version 5.00) and the Command Line Interface (CLI). Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about using the SANsurfer Switch Manager application. Refer to Appendix B Command Line Interface for more information about the command line interface.

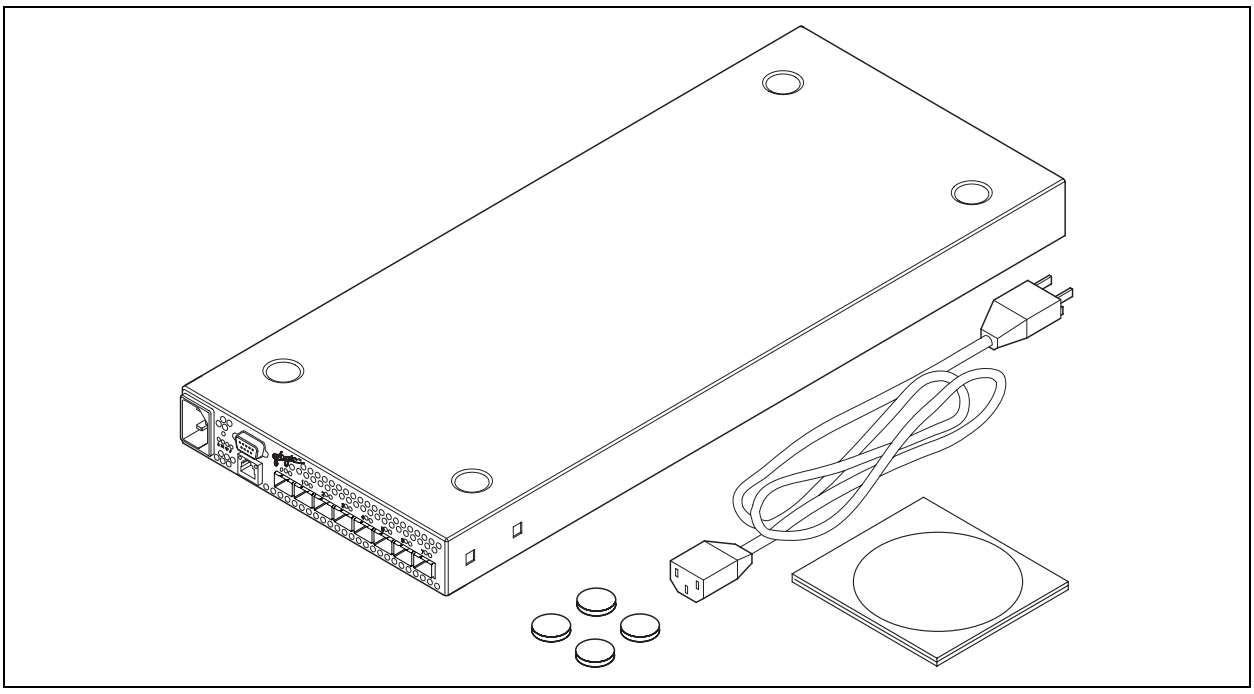


Figure 2-1. SANbox2-8c Fibre Channel Switch

2.1 Chassis Controls and LEDs

The Maintenance button shown in Figure 2-2 is the only chassis control and is used to reset a switch or to recover a disabled switch. The chassis LEDs provide information about the switch's operational status. These LEDS include the Over Temperature LED, Fan Fail LED, Heartbeat LED, and the Input Power LED. To apply power to the switch, plug the power cord into the switch AC power receptacle and into a 110 or 230 VAC power source.

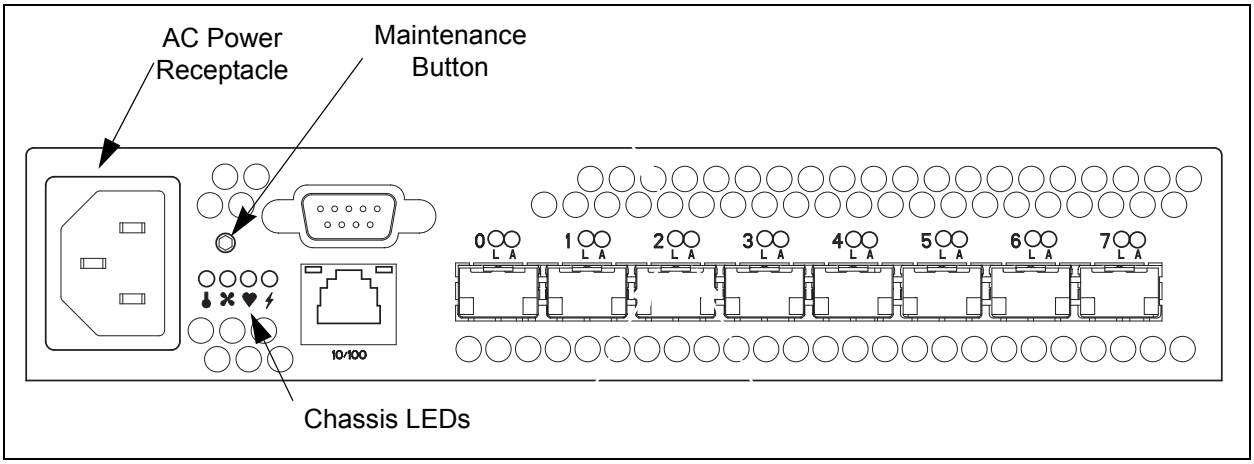


Figure 2-2. Chassis Controls and LEDS

2.1.1 Maintenance Button

The Maintenance button is a dual-function momentary switch on the front panel. Its purpose is to reset the switch or to place the switch in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes when flash memory or the resident configuration file is corrupted. Refer to “Recovering a Switch” on page 5-11 for more information about using maintenance mode.

2.1.1.1 Resetting a Switch

To reset the switch, use a pointed tool to momentarily press and release (less than 2 seconds) the Maintenance button. The switch will respond as follows:

1. All of the chassis LEDs will illuminate and then extinguish leaving only the Input Power LED illuminated.
2. After approximately 1 minute, the Power-On Self Test (POST) begins illuminating all chassis LEDs.
3. When the POST is complete, the chassis LEDs extinguish leaving the Input Power LED illuminated and the Heartbeat LED flashing once per second.

2.1.1.2 Placing the Switch in Maintenance Mode

To place the switch in maintenance mode, do the following:

1. Isolate the switch from the fabric.
2. Press and hold the Maintenance button with a pointed tool for 2–4 seconds. When the Input Power LED alone is illuminated, release the button.
3. After approximately 1 minute, the POST begins illuminating all chassis LEDs.
4. When the POST is complete, the chassis LEDs extinguish leaving the Input Power LED and the Heartbeat LED illuminated. The Heartbeat LED illuminates continuously while the switch is in maintenance mode.

To exit maintenance mode and return to normal operation, momentarily press and release the Maintenance button to reset the switch.

2.1.2
Chassis LEDs

The chassis LEDs shown in Figure 2-3 provide status information about switch operation. Refer to “Port LEDs” on page 2-6 for information about port LEDs.

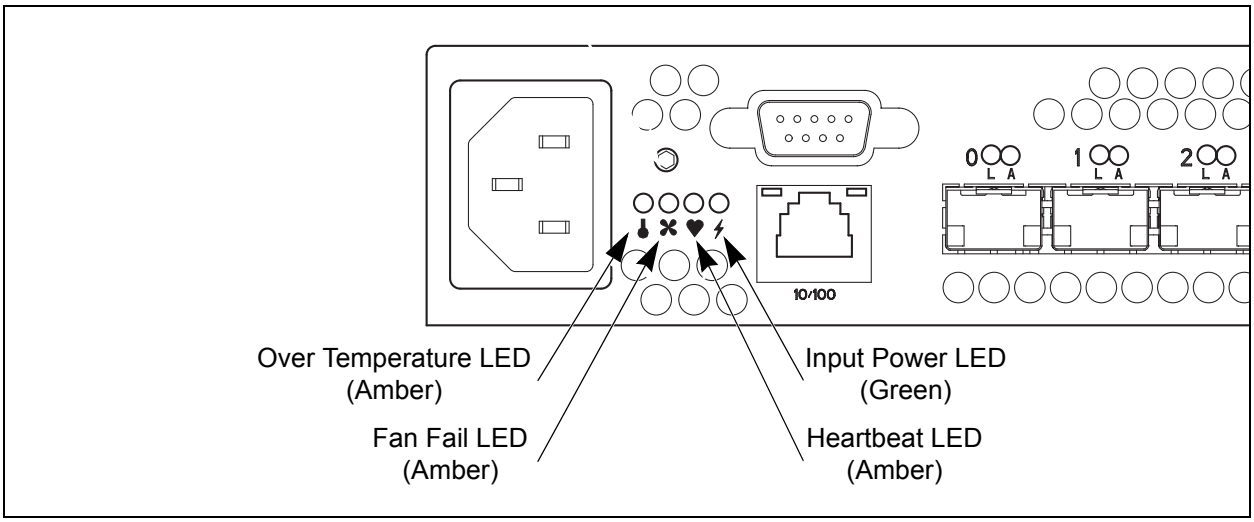


Figure 2-3. Chassis LEDs

2.1.2.1
Over Temperature LED (Amber)

The Over Temperature LED provides status information about the air temperature inside the switch. This LED illuminates to indicate that the switch logic circuitry is overheating. Refer to Section 5 Diagnostics/Troubleshooting for information about troubleshooting over temperature conditions.

2.1.2.2
Fan Fail LED (Amber)

The Fan Fail LED indicates operational status of the fan. This LED illuminates if the speed of the fan falls below the normal range. If the Fan Fail LED illuminates, isolate the switch from the fabric, unplug the switch from the AC power source, and contact your authorized maintenance provider.

2.1.2.3
Heartbeat LED (Amber)

The Heartbeat LED indicates the status of the internal switch processor and the results of the Power On Self Test (POST). Following a normal power-up, the Heartbeat LED blinks about once per second to indicate that the switch passed the POST and that the internal switch processor is running. In maintenance mode, the Heartbeat LED illuminates continuously. Refer to “Heartbeat LED Blink Patterns” on page 5-2 for more information about Heartbeat LED blink patterns.

2.1.2.4
Input Power LED (Green)

The Input Power LED indicates the voltage status at the switch logic circuitry. During normal operation, this LED illuminates to indicate that the switch logic circuitry is receiving the proper DC voltages.

2.2
Fibre Channel Ports

The SANbox2-8c switch has 8 Fibre Channel ports numbered 0–7 as shown in Figure 2-4. Each of these ports is served by a Small Form-Factor Pluggable (SFP) optical transceiver. The port LEDs are located above their respective ports and provide port login and activity status information. The ports self discover the proper mode when connected to public devices and other switches.

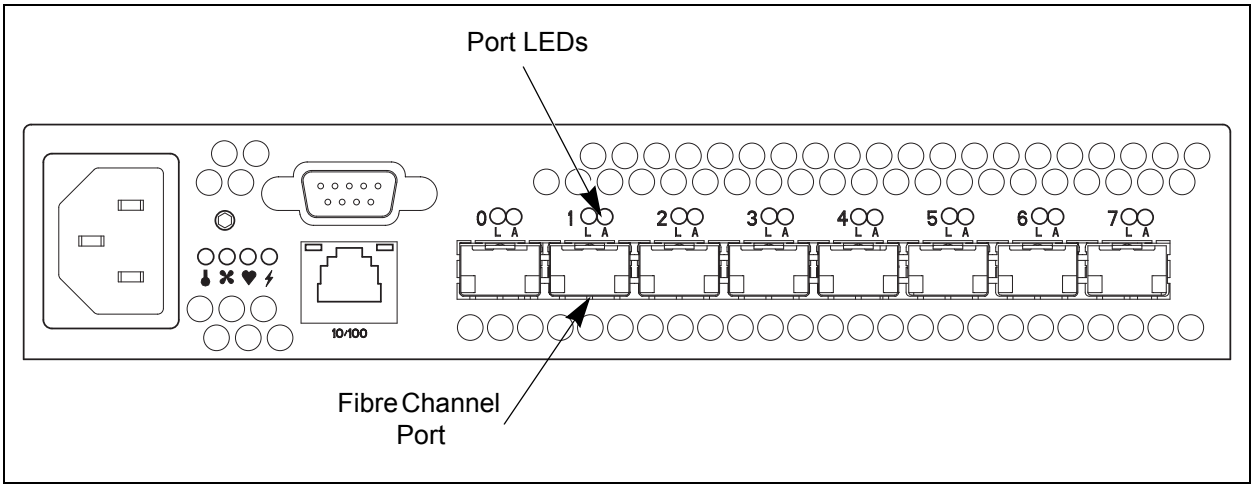


Figure 2-4. Fibre Channel Ports

2.2.1 Port LEDs

Each Fibre Channel port has its own Logged-In LED and Activity LED as shown in Figure 2-5.

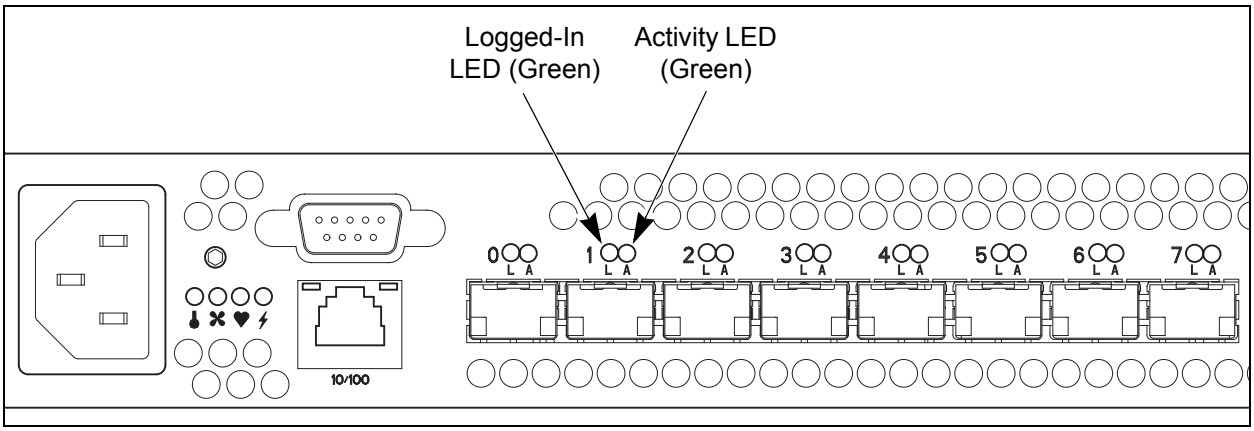


Figure 2-5. Port LEDs

2.2.1.1 Port Logged-In LED

The Logged-in LED indicates the logged-in or initialization status of the connected devices. After successful completion of the POST, the switch extinguishes all Logged-In LEDs. Following a successful loop initialization or port login, the switch illuminates the corresponding logged-in LED. This shows that the port is properly connected and able to communicate with its attached devices. The Logged-In LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Logged-In LED will flash. Refer to “Logged-In LED Indications” on page 5-5 for more information about the Logged-In LED.

2.2.1.2 Port Activity LED

The Activity LED indicates that data is passing through the port. Each frame that the port transmits or receives causes this LED to illuminate for 50 milliseconds. This makes it possible to observe the transmission of a single frame. When extending credits, the Activity LED for a donor port will reflect the traffic of the recipient port. Refer to “Distance” on page 3-4 for more information about extended credits and donor ports.

2.2.2
Small Form-Factor Pluggable (SFP) Transceivers

An SFP transceiver, like the one shown in Figure 2-6, converts electrical signals to and from optical laser signals to transmit and receive. SFP transceivers plug into the ports; duplex fiber optic cables plug into the transceivers which then connect to the devices. A port is capable of transmitting at 1-Gbps or 2-Gbps; however, the transceiver must be capable of 2-Gbps for the port to deliver at that rate.

The SFP transceivers are hot pluggable. This means that you can remove or install an SFP transceiver while the switch is operating without harming the switch or the transceiver. However, communication with the connected device will be interrupted. Refer to "Install SFP Transceivers" on page 4-4 for information about installing and removing SFP optical transceivers.

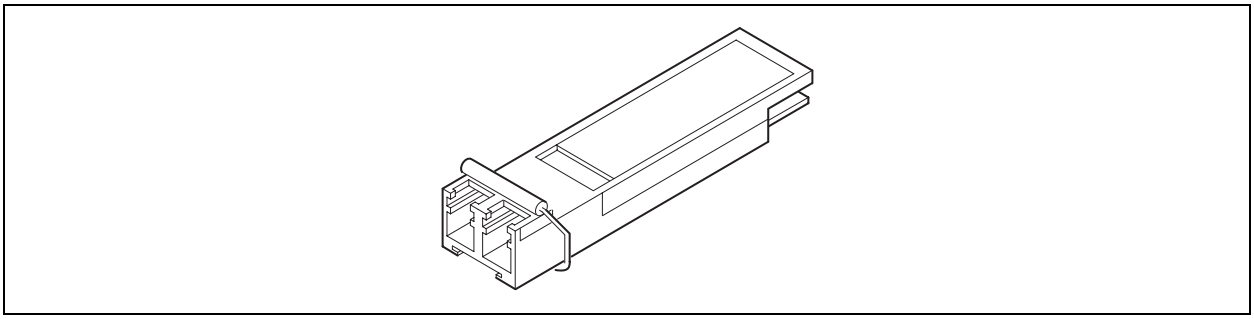


Figure 2-6. SFP Transceiver

2.2.3
Port Types

SANbox2-8c switches support generic ports (G_Port, GL_Port), fabric ports (F_Port, FL_Port), and expansion ports (E_Port). Switches come from the factory with all ports configured as GL_Ports. Generic, fabric, and expansion ports function as follows:

- A GL_Port self-configures as an FL_Port when connected to a public loop device, as an F_Port when connected to a single public device, or as an E_Port when connected to another switch. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
- A G_Port self-configures as an F_Port when connected to a single public device, or as an E_Port when connected to another switch.
- An FL_Port supports a loop of up to 126 public devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single public device (N_Port).
- An F_Port supports a single public device.

E_Ports enable you to expand the fabric by connecting SANbox2-8c switches with other switches. SANbox2-8c switches self-discover all inter-switch connections. Refer to “Multiple Chassis Fabrics” on page 3-6 for more information about multiple chassis fabrics. Refer to the *SANbox2-8c/16 Switch Management User’s Guide* for more information about defining port types.

2.3 Ethernet Port

The Ethernet port shown in Figure 2-7 is an RJ-45 connector that provides a connection to a management workstation through a 10/100 Base-T Ethernet cable. A management workstation can be a Windows®, Solaris™, or a Linux®, workstation that is used to configure and manage the switch fabric. You can manage the switch over an Ethernet connection using SANsurfer Switch Manager, the Command Line Interface (CLI), or SNMP. The switch through which the fabric is managed is called the fabric management switch.

The Ethernet port has two LEDs: the Link Status LED (green) and the Activity LED (amber). The Link Status LED illuminates continuously when an Ethernet connection has been established. The Activity LED illuminates when data is being transmitted or received over the Ethernet connection.

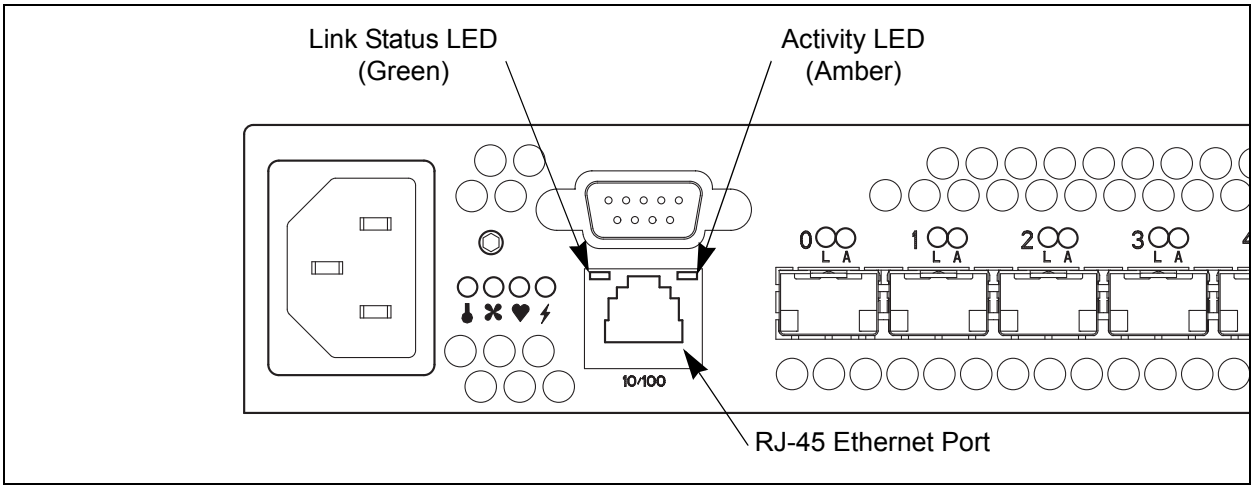


Figure 2-7. Ethernet Port

2.4 Serial Port

The SANbox2-8c switch is equipped with an RS-232 serial port for maintenance purposes. The serial port location is shown in Figure 2-8. You can manage the switch through the serial port using the CLI.

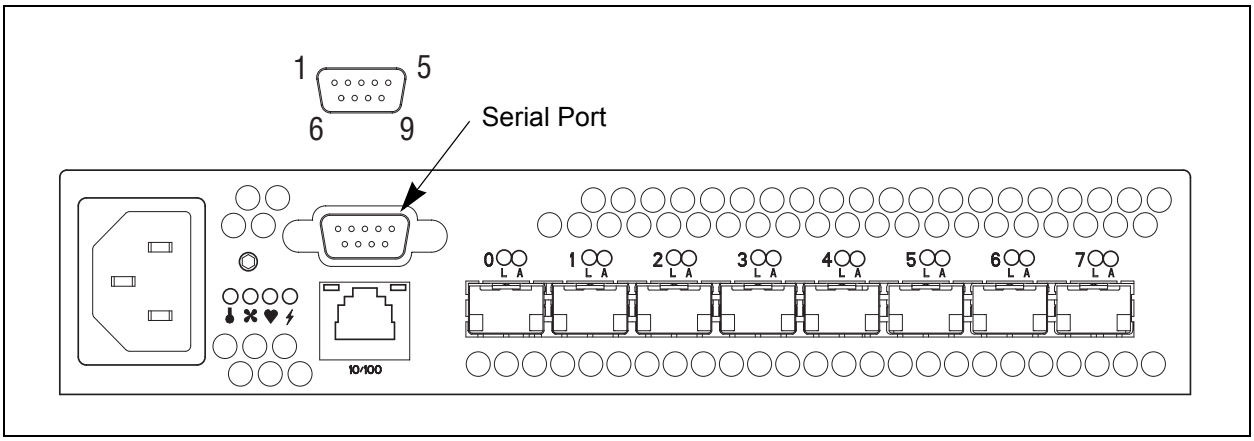


Figure 2-8. Serial Port and Pin Identification

The serial port connector requires a null-modem F/F DB9 cable. The pins on the switch RS-232 connector are shown in Figure 2-8 and identified in Table 2-1. Refer to "Connect the Workstation to the Switch" on page 4-5 for information about connecting the management workstation through the serial port.

Table 2-1. Serial Port Pin Identification

Pin Number	Description
1	Carrier Detect (DCD)
2	Receive Data (RxD)
3	Transmit Data (TxD)
4	Data Terminal Ready (DTR)
5	Signal Ground (GND)
6	Data Set Ready (DSR)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	Ring Indicator (RI)

2.5 Power Supply and Fan

The power supply converts standard 110 or 230 VAC to DC voltages for the various switch circuits. An internal fan provides cooling. Air flow can be front-to-back or back-to-front depending on the switch model. To energize the switch, plug the power cord into the switch AC receptacle and into a 110 or 230 VAC power source.

Note: The power supply and fan are not field replaceable units.

2.6 Switch Management

The switch supports the following management tools:

- SANsurfer Switch Manager
- SANsurfer Switch Manager Web Applet
- Command Line Interface
- SANsurfer Switch Manager Application Programming Interface
- Simple Network Management Protocol
- File Transfer Protocol

2.6.1 SANsurfer Switch Manager

SANsurfer Switch Manager is a workstation-based Java® application that provides a graphical user interface for fabric management. This includes SANsurfer Performance Viewer which graphs port performance. SANsurfer Switch Manager can run on a Windows, Solaris, or Linux workstation. A management workstation connects to the fabric through the Ethernet port of one or more switches and can provide in-band management for all other switches in the fabric. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about the SANsurfer Switch Manager application and its use.

2.6.2 SANsurfer Switch Manager Web Applet

To make switch management less dependent on a particular workstation, each switch contains a SANsurfer Switch Manager web applet. One instance of the web applet can be run at a time by opening the switch IP address with an internet browser. The switch comes from the factory with the web applet enabled, but you can disable it using the EmbeddedGUIEnabled parameter of the Set Setup System command.

The applet possesses the same features as the workstation-based version with the following exceptions:

- Extended Credits wizard
- Zoning Wizard
- SANsurfer Performance Viewer
- Condensed online help

2.6.3 Command Line Interface

The command line interface (CLI) provides monitoring and configuration functions by which the administrator can manage the fabric and its switches. The CLI is available over an Ethernet connection or a serial connection. Refer to Appendix B Command Line Interface for more information.

2.6.4 SANsurfer Switch Manager Application Programming Interface

The SANsurfer Switch Manager API enables an application provider to build a management application for QLogic switches. The library is implemented in ANSI standard C, relying only on standard POSIX run-time libraries (except for the Windows NT build). Contact your distributor or authorized reseller for information about the SANsurfer Switch Manager API.

2.6.5 Simple Network Management Protocol

SNMP provides monitoring and trap functions for the fabric. SANbox2 firmware supports SNMP versions 1 and 2, the Fibre Alliance Management Information Base (FA-MIB) version 4.0, and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps can be formatted using SNMP version 1 or 2. Refer to the *SANbox/SANbox2 Simple Network Management Protocol Reference Guide* for more information about using SNMP.

2.6.6
File Transfer Protocol

FTP provides the command line interface for exchanging files between the switch and the management workstation. These files include firmware image files, configuration files, and log files. “Backing up and Restoring Switch Configurations” on page B-4 provides an example of using FTP to transfer configuration files.

Section 3

Planning

Consider the following when planning a fabric:

- Devices
- Device Access
- Performance
- Multiple Chassis Fabrics
- Switch Services
- Fabric Security
- Fabric Management

3.1 Devices

When planning a fabric, consider the number of devices and the anticipated demand. This will determine the number of ports that are needed and the number of switches. Consider how many and what types of switches are needed.

The switch uses SFP transceivers, but the device host bus adapters you are using may not. Consider whether the device adapters use SFP transceivers or Gigabit Interface Converters (GBIC), and choose fiber optic cables accordingly. Use LC-type cable connectors for SFP transceivers and SC-type cable connectors for GBIC transceivers. Also, consider the transmission speed compatibility of your devices, HBAs, switches, SFPs.

SANbox2 switches support public initiator and target devices. Consider the distribution of target and initiator devices. An F_Port supports a single public device. An FL_Port can support up to 126 public devices in an arbitrated loop.

3.2 Device Access

Consider device access needs within the fabric. Access is controlled by the use of zones and zone sets. Some zoning strategies include the following:

- Group devices by operating system.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Reserve a path and its bandwidth from one port to another.

A zone is a named group of devices that can communicate with each other. Membership in a zone can be defined by switch domain ID and port number, port Fibre Channel address, or by device worldwide name (WWN). Devices can communicate only with devices within the same zone. The SANbox2-8c switch supports both hard and soft zones. A zone can be a member of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

A zoning database is maintained on each switch consisting of all inactive zone sets, the active zone set, all zones, aliases, and their membership. Table 3-1 describes the zoning database limits, excluding the active zone set. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for more information about zoning.

Table 3-1. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256).
MaxZones	Maximum number of zones (1000).
MaxAliases	Maximum number of aliases (2500).
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch's zoning database.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2000), excluding the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

3.2.1
Soft Zones

Soft zoning divides the fabric for purposes of controlling device discovery. Devices in the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. The following rules apply to soft zones:

- Soft zones that include members from multiple switches need not include the ports of the inter-switch links.
- Soft zone boundaries yield to ACL zone boundaries.
- Soft zones can overlap; that is, a port can be a member of more than one soft zone.
- Membership can be defined by Fibre Channel address, domain ID and port number, or port worldwide name.
- Soft zoning supports FL_Ports and F_Ports.

3.2.2
Access Control List Hard Zones

Access Control List (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Members can communicate with each other and transmit outside the ACL zone, but cannot receive inbound traffic from outside the zone. The following rules apply to ACL zones:

- The ACL zone boundary is secure against inbound traffic.
- ACL zones can overlap; that is, a port can be a member of more than one ACL zone.
- ACL zones that include members from multiple switches need not include the ports of the inter-switch links.
- ACL zone boundaries supersede soft zone boundaries.
- Membership can be defined only by domain ID and port ID.

3.3 Performance

The SANbox2-8c switch supports class 2 and class 3 Fibre Channel service with a maximum frame size of 2148 bytes at transmission rates of 1-Gbps or 2-Gbps. A switch port adapts its transmission speed to match that of the device to which it is connected prior to login when the connected device powers up. Related performance characteristics include the following:

- Distance
- Bandwidth
- Latency

3.3.1 Distance

Consider the physical distribution of devices and switches in the fabric. Choose SFP transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. Refer to Appendix A Specifications for more information about cable types and SFP transceivers.

Each port is supported by a data buffer with a 12 credit capacity; that is, 12 maximum sized frames. For fibre optic cables, this enables full bandwidth over a distance of 20 kilometers at 1-Gbps (0.6 credits/Km), or 10 kilometers at 2-Gbps (1.2 credits/Km). Beyond this distance, however, there is some loss of efficiency because the transmitting port must wait for an acknowledgement before sending the next frame.

Longer distances can be spanned at full bandwidth by extending credits on G_Ports and F_Ports. Each port can donate 11 credits to a pool from which a recipient port can borrow. For example, you can configure a recipient port to borrow up to 66 credits from 6 ports for a total of 78 credits. This will support communication over approximately 130 Km at 1 Gbps (78÷0.6) or 65 Km at 2 Gbps (78÷1.2).

You can configure recipient and donor ports using SANsurfer Switch Manager or the Set Config command. Refer to “Set Config Command” on page B-60 for more information.

3.3.2
Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. A port can transmit or receive at nominal rates of 1-Gbps or 2-Gbps depending on the device to which it is connected. This corresponds to actual bandwidth values of 106 MB and 212 MB respectively. Two 1-Gbps source ports can transmit to the same 2-Gbps destination port. Similarly, one 2-Gbps source port can feed two 1-Gbps destination ports.

In multiple chassis fabrics, each link between chassis contributes 106 or 212 MB of bandwidth between those chassis depending on the speed of the link. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch guarantees in-order-delivery with any number of links between chassis.

3.3.3
Latency

Latency is a measure of how fast a frame travels from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship. Port-to-port latency values on the switch are shown in Table 3-2.

Table 3-2. Port-to-Port Latency

	Destination Rate		
Source Rate	**Gbps**	**1**	**2**
	1	< 1 µsec	< 1 µsec[1]
	2	< 0.5 µsec	< 0.4 µsec

[1] Based on minimum sized frame of 36 bytes. Latency increases for larger frame sizes.

3.4 Multiple Chassis Fabrics

By connecting switches together you can expand the number of available ports for devices. Each switch in the fabric is identified by a unique domain ID, and the fabric can automatically resolve domain ID conflicts. Because the Fibre Channel ports are self-configuring, you can connect the SANbox2-8c switch with other switches in a wide variety of topologies.

3.4.1 Optimizing Device Performance

When choosing a topology for a multiple chassis fabric, you should also consider the locality of your server and storage devices and the performance requirements of your application. Storage applications such as video distribution, medical record storage/retrieval or real-time data acquisition can have specific latency or bandwidth requirements.

The SANbox2-8c switch provides the lowest latency of any product in its class. Refer to “Performance” on page 3-4 for information about latency and bandwidth. However, the highest performance is achieved on Fibre Channel switches by keeping traffic within a single switch instead of relying on ISLs. Therefore, for optimal device performance place devices on the same switch under the following conditions:

- Heavy I/O traffic between specific server and storage devices.
- Distinct speed mismatch between devices such as the following:
  - A 2-Gbps server and a slower 1-Gbps storage device
  - A high performance server and slow tape storage device

3.4.2
Domain ID, Principal Priority, and Domain ID Lock

The following switch configuration settings affect multiple chassis fabrics:

- Domain ID
- Principal priority
- Domain ID lock

The domain ID is a unique number from 1–239 that identifies each switch in a fabric. The principal priority is a number (1–255) that determines the principal switch which manages domain ID assignments for the fabric. The switch with the highest principal priority (1 is high, 255 is low) becomes the principal switch. If the principal priority is the same for all switches in a fabric, the switch with the lowest WWN becomes the principal switch.

The domain ID lock allows (False) or prevents (True) the reassignment of the domain ID on that switch. Switches come from the factory with the domain ID set to 1, the domain ID lock set to False, and the principal priority set to 254. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about changing the domain ID and domain ID lock using SANsurfer Switch Manager. Refer to the "Set Config Command" on page B-60 for information about changing the default domain ID, domain ID lock, and principal priority parameters.

An unresolved domain ID conflict means that the switch with the higher WWN will isolate as a separate fabric, and the Logged-In LEDs on both switches will flash green to show the affected ports. If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain ID conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

Note: Domain ID reassignment is not reflected in zoning that is defined by domain ID/port number pair or Fibre Channel address. You must reconfigure zones that are affected by domain ID reassignment. To prevent zoning definitions from becoming invalid under these conditions, lock the domain IDs using SANsurfer Switch Manager or the Set Config Switch command.

3.4.3
Common Topologies

The SANbox2-8c switch supports the following topologies:

- Cascade Topology
- Mesh Topology
- Multistage Topology

3.4.3.1
Cascade Topology

A cascade topology describes a fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology as shown in Figure 3-1. The loop reduces latency because any switch can route traffic in the shortest direction to any switch in the loop. The loop also provides failover should a switch fail.

The example cascade fabric shown in Figure 3-1 has the following characteristics:

- Each chassis link contributes up to 200 MB/s of bandwidth between chassis, 400 MB/s in full duplex. However, because of the sequential structure, that bandwidth will be shared by traffic between devices on other chassis.
- Latency between any two ports is no more than two chassis hops.
- 24 Fibre Channel ports are available for devices.

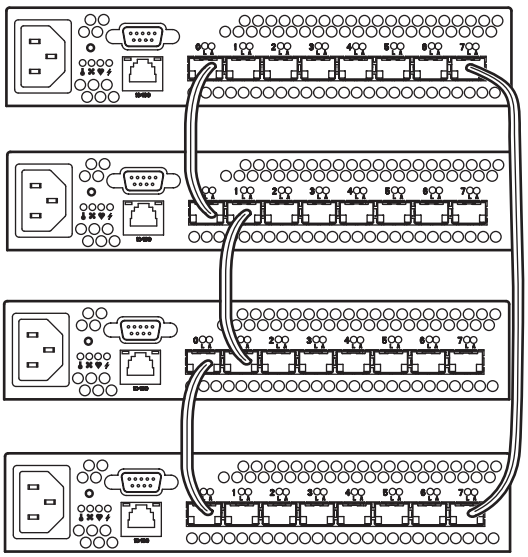


Figure 3-1. Cascade-with-a-Loop Topology

3.4.3.2

Mesh Topology

A mesh topology describes a fabric in which each chassis has at least one port directly connected to each other chassis in the fabric. The example mesh fabric shown in Figure 3-2 has the following characteristics:

- Each link contributes up to 200 MB/s of bandwidth between switches, 400 MB/s in full duplex. Because of multiple parallel paths, there is less competition for this bandwidth than with a cascade or a Multistage topology.
- Latency between any two ports is one chassis hop.
- 20 Fibre Channel ports are available for devices.

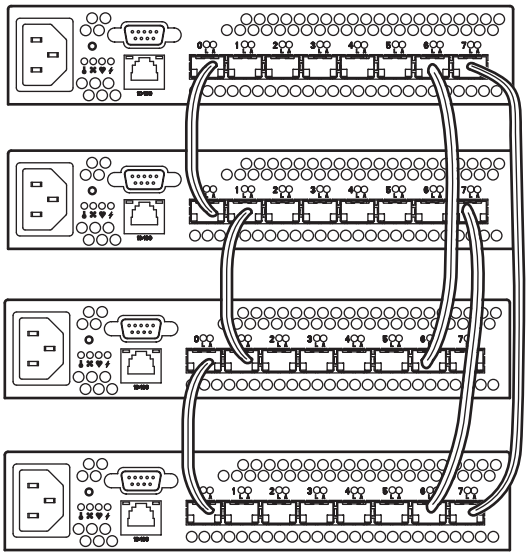


Figure 3-2. Mesh Topology

3.4.3.3

Multistage Topology

A Multistage® topology describes a fabric in which two or more edge switches connect to one or more core switches. The Multistage fabric shown in Figure 3-3 has the following characteristics:

- Each link contributes up to 200 MB/s of bandwidth between chassis. Competition for this bandwidth is less than that of a cascade topology, but greater than that of the mesh topology.
- Latency between any two ports is no more than two chassis hops.
- 26 Fibre Channel ports are available for devices

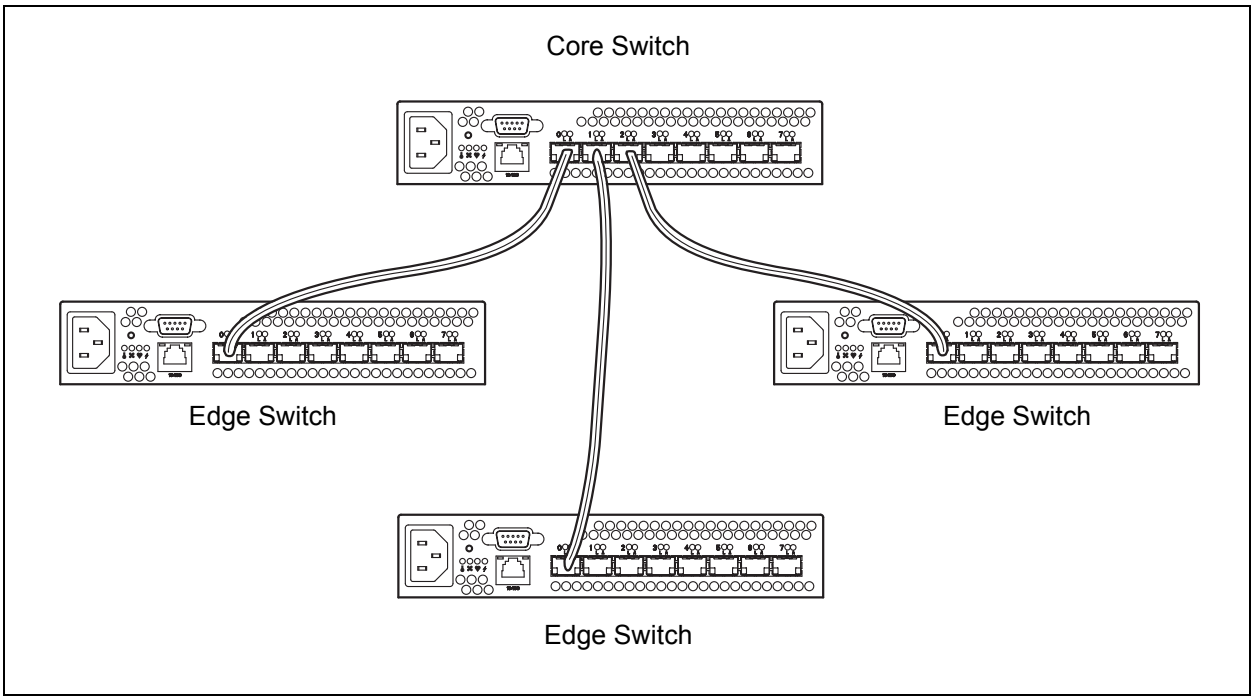


Figure 3-3. Multistage Topology

3.5 Switch Services

You can configure your switch to suit the demands of your environment by enabling or disabling a variety of switch services. Familiarize yourself with the following switch services and determine which ones you need:

- **Telnet**: Provides for the management of the switch over a Telnet connection. Disabling this service is not recommended. The default is enabled.
- **Secure Shell (SSH)**: Provides for secure remote connections to the switch using SSH. Your workstation must also use an SSH client. The default is disabled.
- **Switch Management**: Provides for out-of-band management of the switch with SANsurfer Switch Manager, the SANsurfer Switch Manager Application Application Programming Interface, SNMP, and CIM. If this service is disabled, the switch can only be managed inband or through the serial port. The default is enabled.
- **Inband Management**: Provides for the management of the switch over an inter-switch link using SANsurfer Switch Manager, SNMP, management server, or the application programming interface. If you disable inband management, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection.The default is enabled.
- **Secure Socket Layer (SSL)**: Provides for secure SSL connections for SANsurfer Switch Manager, the SANsurfer Switch Manager web applet, SANsurfer Switch Manager Application Programming Interface, and CIM. This service must be enabled to authenticate users through a RADIUS server when using SANsurfer Switch Manager. To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. Enabling SSL automatically creates a security certificate on the switch. The default is enabled.
- **SANsurfer Switch Manager web applet**: Provides for access to the SANsurfer Switch Manager web applet. The web applet enables you to point at a switch with an internet browser and run SANsurfer Switch Manager through the browser. The default is enabled.
- **Simple Network Management Protocol (SNMP)**: Provides for the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). Security consists of a read community string and a write community string that serve as passwords that control read and write access to the switch. These strings are set at the factory to these well-known defaults and should be changed if SNMP is to be enabled. Otherwise, you risk unwanted access to the switch. The default is enabled.

- **Network Time Protocol (NTP)**: Provides for the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is disabled.
- **Common Information Model (CIM)**: Provides for the management of the switch through third-party applications that use CIM. The default is enabled.
- **File Transfer Protocol (FTP)**: Provides for transferring files rapidly between the workstation and the switch using FTP. The default is enabled.
- **Management Server (MS)**: Enables or disables the management of the switch through third-party applications that use GS-3 Management Server. The default is disabled.

3.6 Fabric Security

An effective security profile begins with a security policy that states the requirements. A threat analysis is needed to define the plan of action followed by an implementation that meets the security policy requirements. Internet portals, such as remote access and email, usually present the greatest threats. Fabric security should also be considered in defining the security policy.

Most fabrics are located at a single site and are protected by physical security, such as key-code locked computer rooms. For these cases, security methods such as user passwords for equipment and zoning for controlling device access, are satisfactory.

Fabric security is needed when security policy requirements are more demanding: for example, when fabrics span multiple locations and traditional physical protection is insufficient to protect the IT infrastructure. Another benefit of fabric security is that it creates a structure that helps prevent unintended changes to the fabric.

Fabric security consists of the following:

- Connection Security
- Device Security
- User Account Security

3.6.1
Connection Security

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the command line interface and the Secure Socket Layer (SSL) protocol for management applications such as SANsurfer Switch Manager and Common Information Module (CIM).

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. When the SSL service is enabled, a certificate is automatically created on the switch. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to snychronize the workstation and switch with the same date, time, and time zone. The switch certificate is valid 24 hours before its creation date and 365 days after its creation date. If the certificate should become invalid, refer to the “Create Command” on page B-19 for information about creating a certificate.

Consider your requirements for connection security: for the command line interface (SSH), management applications such as SANsurfer Switch Manager (SSL), or both. If SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize workstations and switches.

- Refer to System keyword of the “Set Setup Command” on page B-77 for information about enabling the NTP client on the switch and configuring the NTP server.
- Refer to the “Set Command” on page B-58 for information about setting the time zone.

3.6.2
Device Security

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS). A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of groups is 16.
- Maximum number of members in a group is 1000.
- Maximum total number of group members is 1000.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch's security database, or remotely using a Remote Dial-In User Service (RADIUS) server such as Microsoft® RADIUS. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts as described in "User Account Security" on page 3-24. A secure connection is required to authenticate user logins with a RADIUS server. Refer to "Connection Security" on page 3-13 for more information.

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to distributed on the switches or centralized on a RADIUS server and how many servers to configure.

The following examples illustrate how to configure a security database:

- Security Example: Switches and HBAs
- Security Example: RADIUS Server
- Security Example: Host Authentication

3.6.2.1

Security Example: Switches and HBAs

Consider the fabric shown in Figure 3-4. In this fabric, Switch_1, HBA_1, and Switch_2 support security while the JBOD and HBA_2 do not. The objective is to secure F_Ports and E_Ports in the fabric. To do this, configure security on the devices that support security: Switch_1, Switch_2, and HBA_1.

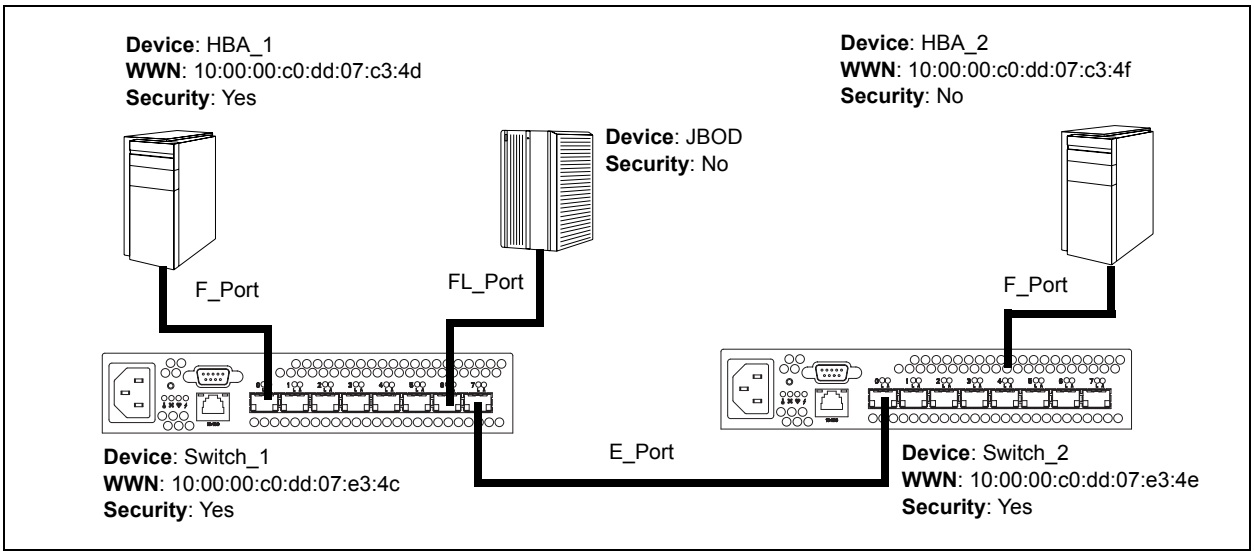


Figure 3-4. Security Example: Switches and HBAs

1. Configure security on Switch_1. Create a security set (Security_Set_1) on Switch_1.
   a. Create a port group (Group_Port_1) in Security_Set_1 with Switch_1 and HBA_1 as members. The JBOD is a loop device, and is therefore, excluded from the port group.

Port Group on Switch_1: Group_Port_1	
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef
HBA_1	Node WWN: 10:00:00:c0:dd:07:c3:4d Authentication: CHAP Primary Hash: MD5 Primary Secret: fedcba9876543210

- You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
- For CHAP authentication, create 32-character hexadecimal or 16-character ASCI secrets. The switch secret must be shared with the HBA security database.

b. Create an ISL group (Group_ISL_1) in Security_Set_1 with Switch_1 and Switch_2 as members. The Switch_1 secret must be shared with the Switch_2 security database.

ISL Group on Switch_1: Group_ISL_1	
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdef abcdef012 Binding: None

2. Configure security on HBA_1 using the appropriate management tool. Logins between the Switch_1 and HBA_1 will be challenged for their respective secrets. Therefore, the secrets for Switch_1 and HBA_1 that you configured on Switch_1 must also be configured on HBA_1.
3. Save Security_Set_1 on Switch_1 and prepare to activate it. Activating a security set does not affect currently logged-in ports. Therefore, to apply the security policy that you designed in the security database, you must offline the secured ports, activate the security set, then place the secured ports back online.

4. Configure security on Switch_2. Create a security set (Security_Set_2) on Switch_2.
   a. Create a port group (Group_Port_2) in Security_Set_2. HBA_2 is the only member because HBA_2 does not support authentication.

Port Group on Switch_2: Group_Port_2	
HBA_2	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: None Binding: None

   b. Create an ISL group (Group_ISL_2) in Security_Set_2 with Switch_1 and Switch_2 as members. This is a replication of the entries in ISL group in the Switch_1 security database.

ISL Group on Switch_2: Group_ISL_2	
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Secret: abcdef abcdef012 Binding: None

5. Save Security_Set_2 on Switch_2 and activate it.

3.6.2.2

Security Example: RADIUS Server

Consider the fabric shown in Figure 3-5. This fabric is similar to the one shown in Figure 3-4 with the addition of Radius_1 acting as a RADIUS server. Authorization and authentication is passed from the switch to Radius_1 in the following cases:

- HBA_1 login to Switch_1
- Switch_1 login to Switch_2
- Switch_2 login to Switch_1

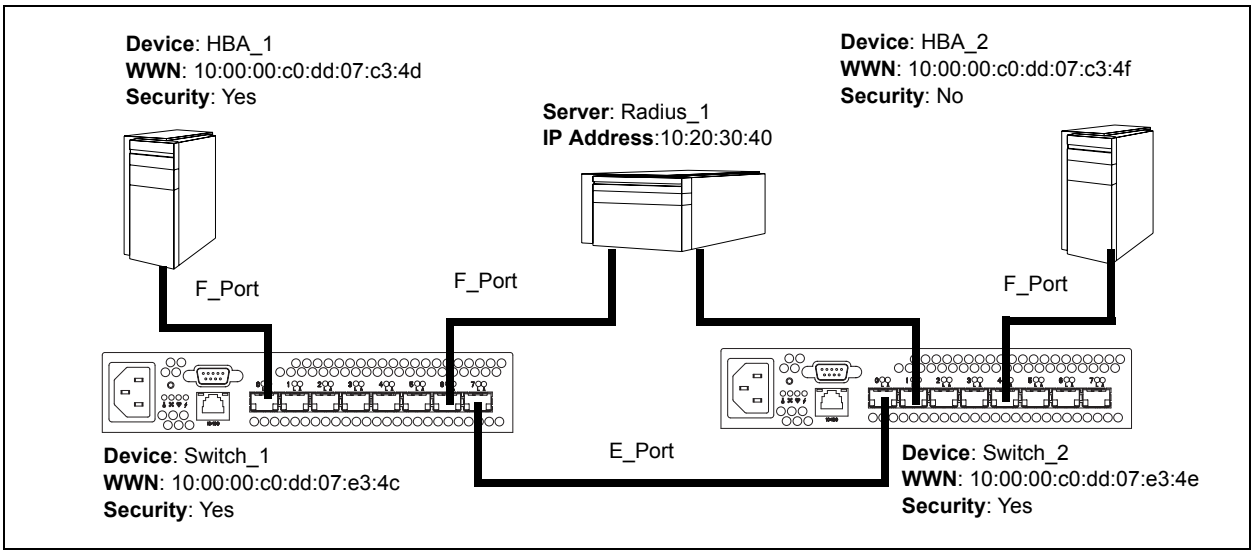


Figure 3-5. Security Example: RADIUS Server

1. Configure the Radius_1 host as a RADIUS server on Switch_1 and Switch_2 to authenticate device logins. Specify the server IP address and the secret with which the switches will authenticate with the server. Configure the switches so that devices authenticate through the switches only if the RADIUS server is unavailable.

Radius_1 Configuration on Switch_1 and Switch_2	
Device Authentication Order	RadiusLocal – Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
Total Servers	1 – Enables support for one RADIUS server
Device Authentication Server	True – Enables Radius_1 to authenticate device logins.
Server IP Address	10.20.30.40
Secret	1234567890123456 – 16-character ASCI string (MD5 hash)

2. Configure security on Switch_1. Create a security set (Security_Set_1) on Switch_1.
   a. Create a port group (Group_Port_1) in Security_Set_1 with Switch_1 and HBA_1 as members. The JBOD is a loop device, and is therefore, excluded from the port group.

Port Group on Switch_1: Group_Port_1	
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef
HBA_1	Node WWN: 10:00:00:c0:dd:07:c3:4d Authentication: CHAP Primary Hash: MD5 Primary Secret: fedcba9876543210

- You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
- For CHAP authentication, create 32-character hexadecimal or 16-character ASCI secrets. The switch secret must be shared with the HBA security database.

b. Create an ISL group (Group_ISL_1) in Security_Set_1 with Switch_1 and Switch_2 as members. The Switch_1 secret must be shared with the Switch_2 security database.

ISL Group on Switch_1: Group_ISL_1	
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdefabcdef012 Binding: None

3. Configure security on HBA_1 using the appropriate management tool. Logins between the Switch_1 and HBA_1 will be challenged (CHAP) for their respective secrets. Therefore, the secrets for Switch_1 and HBA_1 that you configured on Switch_1 must also be configured on HBA_1.
4. Save Security_Set_1 on Switch_1 and prepare to activate it. Activating a security set does not affect currently logged-in ports. Therefore, to apply the security policy that you designed in the security database, you must offline the secured ports, activate the security set, then place the secured ports back online.

5. Configure security on Switch_2. Create a security set (Security_Set_2) on Switch_2.
   a. Create a port group (Group_Port_2) in Security_Set_2. HBA_2 is the only member because HBA_2 does not support authentication.

Port Group on Switch_2: Group_Port_2	
HBA_2	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: None Binding: None

   b. Create an ISL group (Group_ISL_2) in Security_Set_2 with Switch_1 and Switch_2 as members. This is a replication of the entries in ISL group in the Switch_1 security database.

ISL Group on Switch_2: Group_ISL_2	
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdefabcdef0123 Binding: None

6. Save Security_Set_2 on Switch_2 and activate it.

3.6.2.3

Security Example: Host Authentication

Consider the fabric shown in Figure 3-6. In this fabric, only Switch_2 and HBA_2/APP_2 support security, where APP_2 is a host application. The objective is to secure the management server on Switch_2 from unauthorized access by an HBA or an associated host application.

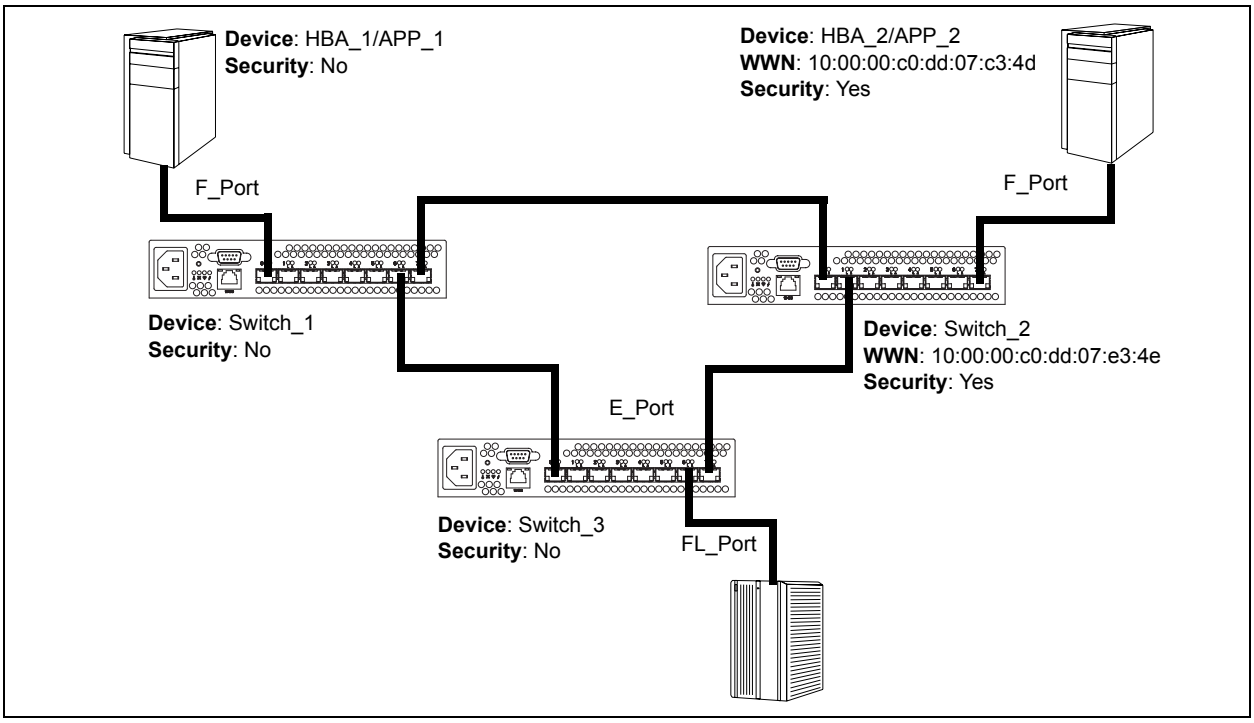


Figure 3-6. Security Example: Management Server

1. Create a security set (Security_Set_2) on Switch_2.
2. Create a Management Server group (Group_1) in Security_Set_2 with Switch_2 and HBA_2 or APP_2 as its member.
   - You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.

- For MD5 authentication, create secrets.

MS Group: Group_1	
Switch_2	Node WWN: 10:00:00:c0:dd:07:c3:4e CT Authentication: True Hash: MD5 Secret: 9876543210fedcba9
HBA_2 or APP_2	Node WWN: 10:00:00:c0:dd:07:c3:4d CT Authentication: True Hash: MD5 Secret: fedcba9876543210

3. Configure security on HBA_2 or APP_2 using the appropriate management tool. Logins between the Switch_2 and HBA_2 or APP_2 will be challenged (MD5) for their respective secrets. Therefore, the secrets that you configured for HBA_2 or APP_2 on Switch_2 must also be configured on HBA_2 or APP_2.
4. Save Security_Set_2 and prepare to activate it. Activating a security set does not affect currently logged-in ports. Therefore, to apply the security policy that you designed in the security database, you must offline the secured ports, activate the security set, then place the secured ports back online.

3.6.3
User Account Security

User account security consists of the administration of account names, passwords, expiration date, and authority level. If an account has Admin authority, all management tasks can be performed by that account in both SANsurfer Switch Manager™ and the Telnet command line interface. Otherwise only monitoring tasks are available. The default account name, Admin, is the only account that can create or change account names and passwords. Account names and passwords are always required when connecting to a switch.

Authentication of the user account and password can be performed locally using the switch's user account database or it can be done remotely using a RADIUS server such as Microsoft® RADIUS. Authenticating user logins on a RADIUS server requires a secure management connection to the switch. Refer to "Connection Security" on page 3-13 for information about securing the management connection. A RADIUS server can also be used to authenticate devices and other switches as described in "Device Security" on page 3-14.

Consider your management needs and determine the number of user accounts, their authority needs, and expiration dates. Also consider the advantages of centralizing user administration and authentication on a RADIUS server.

Note: If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

3.7
Fabric Management

The SANsurfer Switch Manager application and CLI execute on a management workstation that provides for the configuration, control, and maintenance of multiple fabrics. Supported platforms include Windows, Solaris, and Linux. The application can be installed and executed on the workstation, or you can run the SANsurfer Switch Manager web applet that is resident on the switch.

Consider how many fabrics will be managed, how many management workstations are needed, and whether the fabrics will be managed with the CLI, SANsurfer Switch Manager, or the SANsurfer Switch Manager web applet.

A switch supports a combined maximum of 19 logins reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for SANsurfer Switch Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins. Additional logins will be refused.

Notes

Section 4

Installation

This section describes how to install and configure the SANbox2-8c switch. It also describes how to load new firmware and how to recover a disabled switch.

4.1 Site Requirements

Consider the following items when installing a SANbox2-8c switch:

- Fabric Management Workstation
- Switch Power Requirements
- Environmental Conditions

4.1.1 Fabric Management Workstation

The requirements for fabric management workstations running SANsurfer Switch Manager are described in Table 4-1:

Table 4-1. Management Workstation Requirements

Operating System	■ Windows 2000/2003/XP ■ Solaris 8/9/10 ■ Linux® Red Hat® EL 3.x ■ S.u.S.E® Linux 9.0 Enterprise ■ Mac® OS X 10.3
Memory	256 MB or more
Disk Space	150 MB per installation
Processor	500 MHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port, RS-232 serial port (optional)
Internet Browser	Microsoft® Internet Explorer® 5.0 or later Netscape Navigator® 4.72 and later Mozilla™ 1.02 and later Safari® Java 2 Runtime Environment to support web applet

Telnet workstations require an RJ-45 Ethernet port or an RS-232 serial port and an operating system with a Telnet client.

4.1.2
Switch Power Requirements

Power requirements are 1 Amp at 90 to 137 Vac and 0.45 Amps at 180 to 264 Vac.

4.1.3
Environmental Conditions

Consider the factors that affect the climate in your facility such as equipment heat dissipation and ventilation. The switch requires the following operating conditions:

- Operating temperature range: 5 – 50°C (41 – 122°F)
- Relative humidity: 15 – 80%, non-condensing

4.2
Installing a Switch

Unpack the switch and accessories. The SANbox2-8c product is shipped with the components shown in Figure 4-1:

- SANbox2-8c Fibre Channel Switch (1) with firmware installed
- Power cord
- Rubber feet (4)
- CD-ROM containing the SANsurfer Switch Manager switch management application, release notes, and documentation.

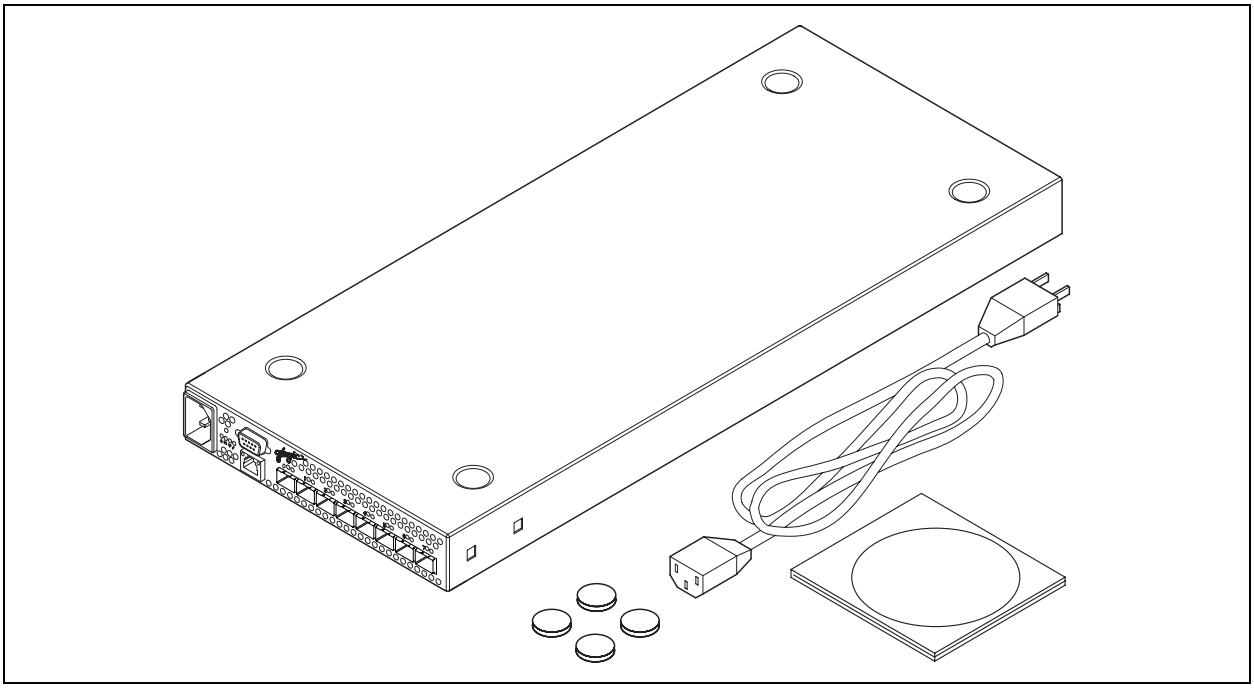


Figure 4-1. SANbox2-8c Fibre Channel Switch

Installing a SANbox2-8c switch involves the following steps:

1. Mount the switch.
2. Install SFP transceivers.
3. Connect the management workstation to the switch.
4. Configure the management workstation.
5. Install the management application.
6. Start the management application.
7. Connect the switch to the AC power source.
8. Configure the switch.
9. Cable devices to the switch.

4.2.1 Mount the Switch

The switch can be placed on a flat surface and stacked or mounted in a 19” EIA rack. Refer to “Dimensions” on page A-3 for weight and dimensional specifications. The top of each chassis has dimples to receive the rubber feet of a second chassis stacked on top. Without the rubber feet, the switch occupies 1U of space in an EIA rack. Mounting rails are required for rack installation and are available through QLogic Corporation.

WARNING!! Mount switches in the rack so that the weight is distributed evenly. An unevenly loaded rack can become unstable possibly resulting in equipment damage or personal injury.

AVERTISSEMENT!!

Installer les commutateurs dans l’armoire informatique de sorte que le poids soit réparti uniformément. Une armoire informatique déséquilibré risque d'entraîner des blessures ou d'endommager l'équipement.

WARNUNG!!

Switches so in das Rack einbauen, dass das Gewicht gleichmäßig verteilt ist. Ein Rack mit ungleichmäßiger Gewichtsverteilung kann schwanken/umfallen und Gerätbeschädigung oder Verletzung verursachen.

CAUTION!

- If the switch is mounted in a closed or multi-unit rack assembly, make sure that the operating temperature inside the rack enclosure does not exceed the maximum rated ambient temperature. Refer to "Environmental" on page A-4.
- The switch must rest on rails or a shelf in the rack or cabinet. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the rack for service access and ventilation.
- Do not restrict chassis air flow. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the rack for service access and ventilation.
- Multiple rack-mounted units connected to the AC supply circuit may overload that circuit or overload the AC supply wiring. Consider the power source capacity and the total power usage of all switches on the circuit. Refer to "Electrical" on page A-3.
- Reliable grounding in the rack must be maintained from the switch chassis to the AC power source.

When mounting the switch in a rack, ensure that the 19-inch rack meets the following standard specifications:

- ANSI/EIA RS-230 Standard, entitled *Cabinets, Racks, Panels, and Associated Equipment*
- MIL-STD- 189, entitled *Racks, Electrical Equipment, 19-Inch and Associated Panels*

4.2.2 Install SFP Transceivers

The switch supports a variety of SFP transceivers. To install a transceiver, insert the transceiver into the port and gently press until it snaps in place. To remove a transceiver, gently press the transceiver into the port to release the tension, then pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver.

Note: The SFP transceiver will fit only one way. If the SFP does not install under gentle pressure, flip it over and try again.

4.2.3
Connect the Workstation to the Switch

You can manage the switch using SANsurfer Switch Manager or the command line interface. SANsurfer Switch Manager requires an Ethernet connection to the switch. The command line interface can use an Ethernet connection or a serial connection. Choose a switch management method, then connect the management workstation to the switch in one of the following ways:

- Indirect Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector through an Ethernet switch or a hub. This requires a 10/100 Base-T straight cable as shown in Figure 4-2.
- Direct Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector. This requires a 10/100 Base-T cross-over cable as shown in Figure 4-2.
- Serial port connection from the management workstation to the switch RS-232 serial port connector. This requires a null modem F/F DB9 cable as shown in Figure 4-2.

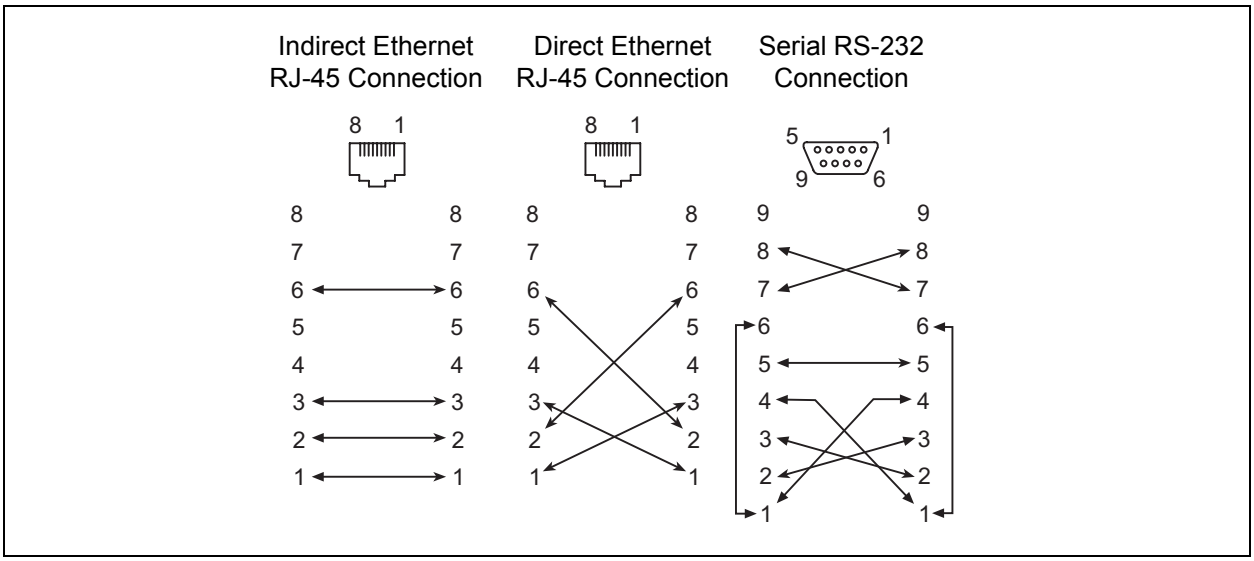


Figure 4-2. Workstation Cable Connections

4.2.4
Configure the Workstation

If you plan to use the command line interface to configure and manage the switch, you must configure the workstation. This involves setting the workstation IP address for Ethernet connections, or configuring the workstation serial port. If you plan to use SANsurfer Switch Manager to manage the switch, the Configuration Wizard manages the workstation IP address for you – proceed to “Install the Management Application” on page 4-8.

4.2.4.1
Setting the Workstation IP Address for Ethernet Connections

The default IP address of a new switch is 10.0.0.1. To ensure that your workstation is configured to communicate with the 10.0.0 subnet, refer to the following instructions for your workstation.

- For a Windows workstation, do the following:
  1. Choose the **Start** button. Choose **Settings**>**Control Panel**>**Network and Dial-Up Connections**.
  2. Choose **Make New Connection**.
  3. Click the **Connect to a private network through the Internet** radio button then click the **Next** button.
  4. Enter 10.0.0.253 for the IP address.
- For a Linux or Solaris workstation, open a command window and enter the following command where (interface) is your interface name:

```
ifconfig (interface) ipaddress 10.0.0.253 netmask 255.255.255.0 up
```

4.2.4.2
Configuring the Workstation Serial Port

To configure the workstation serial port, do the following:

1. Connect a null modem F/F DB9 cable from a COM port on the management workstation to the RS-232 serial port on the switch.
2. Configure the workstation serial port according to your platform:
   - For Windows:
     a. Open the HyperTerminal application. Choose the **Start** button, select **Programs, Accessories, Communications,** and **HyperTerminal**.
     b. Enter a name for the switch connection and choose an icon in the Connection Description window. Choose the **OK** button.
     c. Enter the following COM Port settings in the COM Properties window and choose the **OK** button.
        - ❑ Bits per second: 9600
        - ❑ Data Bits: 8
        - ❑ Parity: None
        - ❑ Stop Bits: 1
        - ❑ Flow Control: None
   - For Linux:
     a. Set up minicom to use the serial port. Create or modify the /etc/minirc.dfl file with the following content:

```
pr portdev/ttyS0
pu minit
pu mreset
pu mhangup
```

     `pr portdev/ttyS0` specifies port 0 on the workstation. Choose "pr" setting to match the workstation port to which you connected the switch.
     b. Verify that all users have permission to run minicom. Review the /etc/minicom.users file and confirm that the line "ALL" exists or that there are specific user entries.
   - For Solaris: Modify the /etc/remote file to include the following lines. /dev/term/a refers to serial port a. Choose the "dv" setting to match the workstation port to which you connected to the switch.

```
SANbox2:
\:dv=/dev/term/a:br#9600:el=^C^S^Q^U^D:ie=%$:oe=^D:
```

3. Proceed to “Connect the Switch to AC Power” on page 4-17.

4.2.5
Install the Management Application

You can manage the switch using SANsurfer Switch Manager as a standalone application or as a part of SANsurfer Management Suite™. SANsurfer Management Suite is QLogic's integrated fabric management application, managing both HBAs and switches.

- If your switch was shipped with a SANsurfer Switch Manager Installation Disk, refer to "SANsurfer Switch Manager" on page 4-8 for instructions on how to install SANsurfer Switch Manager.
- If your switch was shipped with a SANsurfer Management Suite Disk, refer to "SANsurfer Management Suite" on page 4-10 for instructions on how to install SANsurfer Management Suite.

Refer to the *SANbox2-8c/16 Switch Management User's Guide* for more information about using, exiting, and uninstalling SANsurfer Management Suite and SANsurfer Switch Manager.

4.2.5.1
SANsurfer Switch Manager

You can install SANsurfer Switch Manager on a Windows, Linux, Solaris, or Mac OS X® workstation. To install the SANsurfer Switch Manager application from the SANsurfer Switch Manager Installation Disk, do the following:

For a Windows platform:

1. Close all programs currently running, and insert the SANsurfer Switch Manager Installation Disk into the management workstation CD-ROM drive.
2. In the upper left corner of the product introduction screen, click **Management Software**.
3. Locate your platform in the table and click **Install**.

For a Linux platform:

Open the CD and run the installation program with the following path:

```
data/files/Management_Software/Linux/Linux_5.00.xx.xx.bin
```

If there is no CD-ROM icon, do the following:

1. Open an xterm or other terminal window.
2. Mount the CD-ROM. From a shell prompt, enter the following:

   ```
   mount /mnt/cdrom
   ```
3. Change directory to the location of the install program:

   ```
   cd /mnt/cdrom/data/files/Management_Software/Linux
   ```
4. Execute the install program and follow the installation instructions.

   ```
   Linux_5.00.xx.xx.bin
   ```

For a Solaris platform:

1. Open a terminal window. If the disk isn't already mounted, enter the following command:

   ```
   volcheck
   ```

2. Enter following command to move to the directory on the CD that contains the executable:

   ```
   cd /cdrom/cdrom0/data/files/Management_Software/solaris
   ```

3. Execute the install program and follow the installation instructions:

   ```
   Solaris_5.00.xx.xx.bin
   ```

For a Mac OS X platform:

1. Open the CD and move to the following folder:

   ```
   data/files/Management_Software/MacOSX
   ```

2. Double click the applicaton zip file (MacOSX_5.00.xx_xxxx.zip). This will place the install program on your desktop.

3. Locate the **Install** program icon on your desktop, execute it, and follow the installation instructions.

4.2.5.2
SANsurfer Management Suite

The following instructions describe how to install SANsurfer Management Suite and upgrade SANsurfer Switch Manager. You can install SANsurfer Management Suite (SMS) on a Windows, Linux, or Solaris workstation. Choose the instructions for your workstation:

- SMS Installation for Windows
- SMS Installation for Linux
- SMS Installation for Solaris

4.2.5.2.1
SMS Installation for Windows

Close all programs currently running, and insert the SANsurfer Management Suite Installation Disk into the management workstation CD-ROM drive.

1. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Using Windows Explorer, double-click the drive letter which contains the SANsurfer Management Suite Disk.
   b. Locate and double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 Series area.
4. In the Operating System column, click the **Win NT/2000** link.
5. Click the **SANsurfer Management Software** link to open the File Download dialog.
6. You have a choice of running the installation file from the CD-ROM or downloading the installation file to your hard drive. Choose one of the following:
   - Open the installation file from the CD-ROM and follow the SANsurfer Switch Manager installation instructions.
   - Specify a location in which to save the **sansurfer_windows_install.exe** file, and click the **Save** button. Double-click the saved **sansurfer_windows_install.exe** file and follow the installation instructions.

7. When the installation is complete, start SANsurfer Management Suite using the SANsurfer file from the SANsurfer Management Suite installation directory. You can also start SANsurfer Management Suite by clicking the SANsurfer icon (if installed) on the desktop or from the Start menu. In SMS, Click the **Switch** tab in the left pane. From the Help menu, select **About ...** and make note of the version number. Close SANsurfer Management Suite.
8. To ensure that you are using the most recent version of SANsurfer Switch Manager, visit the QLogic support web page and go to Drivers, Software and Manuals.
    a. Select your switch model from the pull-down menu. Locate the description for SANsurfer Switch Manager for Windows under "Management Software".
    b. If the release version number (5.00.xx) is greater than what is currently installed on your workstation, down load the new version and proceed to step 9. Otherwise, no upgrade is needed and the SMS installation is complete.
9. To start the installer, open the zip file and run the **SANsurferSwitchMgr_Windows_5.00.xx.exe** file.
10. When prompted for an installation directory, click the **Choose** button and select the same folder as the SANsurfer Management Suite installation in step 6. The default SMS installation directory is **C:\Program Files\QLogic Corporation\SANsurfer**. Click the Next button.
11. When prompted for the location in which to create the program icons, click the **In an Existing Group** radio button, then specify the same group that was used for the SMS installation. The default SMS group is "QLogic Management Suite". Click the **Next** button.
12. Click the **Install** button to the start the installation. When the installation is complete, click the **Done** button.
13. In the SMS install directory, enter the following command to execute the chglax.bat file. If prompted to overwrite an existing file, enter Y to do so.

    ```
    chglax.bat
    ```

14. Start SANsurfer Switch Manager from SANsurfer Management suite as you did in step 7 and confirm that the new version is running.

4.2.5.2.2
SMS Installation for Linux

Close all programs currently running, and insert the SANsurfer Management Suite Installation Disk into the management workstation CD-ROM drive.

1. If a file browser dialog opens showing icons for the contents of the CD-ROM, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page. If a file browser does not open, double-click the CD-ROM icon to open the browser. If there is no CD-ROM icon, do the following:
   a. Open an xterm or other terminal window.
   b. Mount the CD-ROM. From a shell prompt, enter the following command:
      ```
      mount /mnt/cdrom
      ```
   c. Execute your web browser to view the **Start_Here.htm** document using one of the following commands:
      ```
      mozilla file:/mnt/cdrom/Start_Here.htm
      ```
      or
      ```
      netscape file:/mnt/cdrom/Start_Here.htm
      ```
   d. The SANsurfer Management Suite start page opens in your browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 Series area.
4. In the Operating System column, click the **Linux** link.
5. Click the **SANsurfer Management Software** link to open the File Download dialog.
6. Enter a path name to save the **sansurfer_linux_install.bin** file, and click the **Save** button.
7. Open a terminal window for the directory in which the **sansurfer_linux_install.bin** file was saved, and make the file executable.
   ```
   chmod +x sansurfer_linux_install.bin
   ```
8. Execute the install program and follow the installation instructions
   ```
   ./sansurfer_linux_install.bin
   ```
9. When the installation is complete, start SANsurfer Management Suite using the SANsurfer file in the installation directory. Click the **Switch** tab from the left pane to open SANsurfer Switch Manager. From the Help menu, select **About ...** and make note of the release version number. Close SANsurfer Management Suite.

10. To ensure that you are using the most recent version of SANsurfer Switch Manager, visit the QLogic support web page and go to Drivers, Software and Manuals.
    a. Select your switch model from the pull-down menu. Locate the description for SANsurfer Switch Manager for Linux under "Management Software".
    b. If the release version number (5.00.xx) is greater than what is currently installed on your workstation, down load the new version and proceed to step 11. Otherwise, no upgrade is needed and the SMS installation is complete.
11. From the tar.gz file, extract the **SANsurferSwitchMgr_Linux_5.00.xx.bin** file and make the file executable.

    ```
    chmod +x sansurferswitchmgr_linux_5.00.xx.bin
    ```

12. Execute the install program and follow the installation instructions.

    ```
    ./sansurferswitchmgr_linux_5.00.xx.bin
    ```

13. When prompted for an installation directory, click the **Choose** button and select the same folder as the SANsurfer Management Suite installation in step 9. The default SMS installation directory is /opt/QLogic_Corporation/SANsurfer.
14. Enter the following script command from the installation directory:

    ```
    ./chglax
    ```

15. Start SANsurfer Switch Manager from SANsurfer Management suite as you did in step 9 and confirm that the new version is running.

4.2.5.2.3

SMS Installation for Solaris

To install the SANsurfer Switch Manager application on Solaris from the SANsurfer Management Suite CD-ROM, do the following:

1. Insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Right-click the Workspace Menu.
   b. Select **File**, then select **File Manager**.
   c. In File Manager, double-click the CD-ROM folder, and then double-click the Sansurfer folder.
   d. In the Sansurfer folder, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 Series area.
4. In the Operating System column, click the **Solaris SPARC** link.
5. Click the **SANsurfer Management Software** link to open the Save As dialog.
6. Enter a path name to save the **sansurfer_solaris_install.bin** file and click the **Save** button.
7. Open a terminal window for the directory in which the **sansurfer_solaris_install.bin** file was saved, and enter the following:

   ```
   chmod +x sansurfer_solaris_install.bin
   ```

8. Execute the install program and follow the installation instructions:

   ```
   ./sansurfer_solaris_install.bin
   ```

9. When the installation is complete, start SANsurfer Management Suite using the SANsurfer file in the installation directory. Click the **Switch** tab from the left pane to open SANsurfer Switch Manager. From the Help menu, select **About ...** and make note of the release version number. Close SANsurfer Management Suite.

10. To ensure that you are using the most recent version of SANsurfer Switch Manager, visit the QLogic support web page and go to Drivers, Software and Manuals.
    a. Select your switch model from the pull-down menu. Locate the description for SANsurfer Switch Manager for Linux under "Management Software".
    b. If the release version number (5.00.xx) is greater than what is currently installed on your workstation, down load the new version. Otherwise, no upgrade is needed.
11. Open the tar file and save the **SANsurferSwitchMgr_QLGCsol_5.00.xx.bin** file in a folder and make the file executable.

    ```
    # chmod +x sansurferswitchmgr_QLGCsol_5.00.xx
    ```

12. Install the new SANsurfer Switch Manager package:

    ```
    # pkgadd -d sansurferswitchmgr_QLGCsol_5.00.xx
    ```

13. Change directories to the package location:

    ```
    # cd /usr/opt/QLGCsol/bin
    ```

14. Locate and execute the file **sbm_over_sms.sh**:

    ```
    # ./sbm_over_sms.sh
    ```

15. When prompted for the SMS installation directory, enter **d** if SMS was installed in it's default directory (/opt/QLogic_Corporation/SANsurfer). Otherwise, enter the path name for the SMS installation directory. The script will copy the necessary files to the specified installation directory.
16. Start SANsurfer Switch Manager from SANsurfer Management suite as you did in step 9 and confirm that the new version is running.

4.2.6
Start SANsurfer Switch Manager

You can start SANsurfer Switch Manager as a standalone application or from SANsurfer Management Suite.

Note: After the switch is operational, you can also open the SANsurfer Switch Manager web applet, by entering the switch IP address in an internet browser. If your workstation does not have the Java 2 Run Time Environment program, you will be prompted to download it.

- To start SANsurfer Switch Manager as a standalone application, do the following.
  1. Start the SANsurfer Switch Manager using one of the following methods:
     - For Windows, double-click the SANsurfer Switch Manager shortcut, or select SANsurfer Switch Manager from Start menu, depending on how you installed the SANsurfer Switch Manager application. From a command line, you can enter the SANsurfer_Switch_Manager command:

       ```
       <install_directory>SANsurfer_Switch_Manager.exe
       ```

     - For Linux, Solaris, or Mac OS X, enter the following command:

       ```
       <install_directory>./SANsurfer_Switch_Manager
       ```

  2. In the Initial Start dialog, click the **Open Configuration Wizard** button. When you power up the switch, the Configuration Wizard will recognize the switch and lead you through the configuration process.
- To start SANsurfer Switch Manager from SANsurfer Management Suite, do the following.
  1. Start the SANsurfer Management Suite application using one of the following methods:
     - For Windows, double-click the SANsurfer shortcut, or select **SANsurfer** from Start menu, depending on how you installed the SANsurfer application. From a command line, enter the following command:

       ```
       <install_directory>\SANsurfer.exe
       ```

     - For Linux or Solaris enter the SANsurfer command:

       ```
       <install_directory>./SANsurfer
       ```

  2. From the SANsurfer Management Suite home page, click the SANsurfer Switch Manager button.

3. In the Initial Start dialog, click the **Open Configuration Wizard** button. When you power up the switch, the Configuration Wizard will recognize the switch and lead you through the configuration process.

4.2.7 Connect the Switch to AC Power

WARNING!! This product is supplied with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded outlet to avoid electrical shock. An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the switch chassis. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent electrical shock.

You may require a different power cable in some countries because the plug on the cable supplied with the equipment will not fit your electrical outlet. In this case, you must supply your own power cable. The cable you use must meet the following requirements:

- For 125 Volt electrical service, the cable must be rated at 10 Amps and be approved by UL and CSA.
- For 250 Volt electrical service: The cable must be rated at 10 Amps, meet the requirements of H05VV-F, and be approved by VDE, SEMKO, and DEMKO.

AVERTISSEMENT!!

Pour la sécurité de l'utilisateur, l'appareil est livré avec un câble d'alimentation trifilaire et une fiche. Pour éviter toute secousse électrique, enficher ce câble à une prise correctement mise à la terre.Une prise électrique dont les fils sont mal branchés peut créer une tension dangereuse dans les pièces métalliques du châssis switch. Pour éviter toute secousse électrique, s'assurer que les fils sont correctement branchés et que la prise est bien mise à la terre.

Dans certains pays les prises électriques sont de modèle différent; on ne peut y enficher le câble de l'appareil. On doit donc en utiliser un autre ayant les caractéristiques suivantes:

- Alimentation 125 V: Câble pour courant nominal de 10 A, agréé LAC et CSA.
- Alimentation 250 V: Câble pour courant nominal de 10 A, conforme au H05VV-F, et agréé VDE, SEMKO et DEMKO.

WARNUNG!!

Dieses Produkt wird mit einem 3-adrigen Netzkabel mit Stecker geliefert. Dieses Kabel erfüllt die Sicherheitsanforderungen und sollte an einer vorschriftsmäßigen Schukosteckdose angeschlossen werden, um die Gefahr eines elektrischen Schlages zu vermeiden.Elektrosteckdosen, die nicht richtig verdrahtet sind, können gefährliche Hochspannung an den Metallteilen des switch-Gehäuses verursachen. Der Kunde trägt die Verantwortung für eine vorschriftsmäßige Verdrahtung und Erdung der Steckdose zur Vermeidung eines elektrischen Schlages.

In manchen Ländern ist eventuell die Verwendung eines anderen Kabels erforderlich, da der Stecker des mitgelieferten Kabels nicht in die landesüblichen Steckdosen paßt. In diesem Fall müssen Sie sich ein Kabel besorgen, daß die folgenden Anforderungen erfüllt:

- Für 125 Volt-Netze: 10 Ampere Kabel mit UL- und CSA-Zulassung.
- Für 250 Volt-Netze: 10 Ampere Kabel gemäß den Anforderungen der H05VV-F und VDE-, SEMKO- und DEMKO-Zulassung.

To energize the switch, connect the power cord to the AC power receptacle on the front of the switch chassis and to a grounded AC outlet. The switch responds in the following sequence:

1. The chassis LEDs (Fan Fail, Over Temperature, Heartbeat, Input Power) illuminate followed by all port Logged-In LEDs.
2. After a couple seconds, the Over Temperature, Fan Fail, and Heartbeat LEDs are extinguished while the Input Power LED remains illuminated.
3. After approximately one minute, the POST executes and all LEDs illuminate.
4. When the POST is complete, all LEDs are extinguished except the Input Power LED and the Heartbeat LED:
   - The Input Power LED remains illuminated indicating that the switch logic circuitry is receiving DC voltage. If not, contact your authorized maintenance provider.

- The Heartbeat LED indicates the results of the POST. The POST tests the condition of firmware, memories, data-paths, and switch logic circuitry. If the Heartbeat LED blinks steadily about once per second, the POST was successful, and you can continue with the installation process. Any other blink pattern indicates that an error has occurred. Refer to “Heartbeat LED Blink Patterns” on page 5-2 for more information about error blink patterns.

The application opens with the Initial Start dialog. Refer to the *SANbox2-8c/16 Switch Management User’s Guide* for more information about using, exiting, and uninstalling SANsurfer Switch Manager.

4.2.8 Configure the Switch

You can configure the switch using the SANsurfer Switch Manager application or the command line interface. To configure the switch using SANsurfer Switch Manager, click the **Open Configuration Wizard** radio button in the Initial Start dialog, then click the **Proceed** button. The Configuration wizard explains and prompts you for the following configuration information:

Temporary IP address	
Temporary subnet mask	
Archive template file	
Switch domain ID (1–-239)	
Domain ID Lock (Locked/Unlocked)	
Switch name	
Permanent IP address	
Permanent subnet mask	
Permanent gateway address	
Permanent network discovery method	
Date and time	
Admin account password	
Create a configuration archive?	

Note: Refer to Table B-9 through Table B-16 for information on factory configuration default values.

To configure the switch using the command line interface, do the following:

1. Open a command window according to the type of workstation and connection:
   - Ethernet (all platforms): Open a Telnet session with the default switch IP address and log in to the switch with default account name and password (admin/password).

     ```
     telnet 10.0.0.1
     Switch Login: admin
     Password:     *******
     ```

   - Serial – Windows: Open the HyperTerminal application on a Windows platform.
     a. Choose the **Start** button, select **Programs, Accessories, HyperTerminal,** and **HyperTerminal**.
     b. Select the connection you created earlier and choose the **OK** button.
   - Serial – Linux: Open a command window and enter the following command:

     ```
     minicom
     ```

   - Serial – Solaris: Open a command window and enter the following command:

     ```
     tip sanbox2
     ```

2. Open an admin session and enter the Set Setup System command. Enter the values you want for switch IP address (Eth0NetworkAddress) and the network mask (Eth0NetworkMask). Refer to "Set Setup Command" on page B-77 for more information about this command.

   ```
   SANbox2 #> admin start
   SANbox2 (admin) #> set setup system
   ```

3. Open a Config Edit session and use the Set Config command to modify the switch configuration. Refer to the "Config Command" on page B-16 and the "Set Config Command" on page B-60 for more information.

4.2.9 Cable Devices to the Switch

Connect cables to the SFP transceivers and their corresponding devices, and then energize the devices. Device host bus adapters can have SFP (or SFF) transceivers or GigaBit Interface Converters (GBIC). LC-type duplex fiber optic cable connectors are designed for SFP transceivers, while SC-type connectors are designed for GBICs. Duplex cable connectors are keyed to ensure proper orientation. Choose the fiber optic cable with the connector combination that matches the device host bus adapter.

GL_Ports self configure as FL_Ports when connected to loop of public devices or F_Ports when connected to a single device. G_Ports self configure as F_Ports when connected to single public devices. Both GL_Ports and G_Ports self configure as E_Ports when connected to another switch.

4.3 Install Firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. You can use the SANsurfer Switch Manager application or the CLI to install new firmware.

Note: You can load and activate version 5.0 firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the switch will perform a disruptive activation:

- The current firmware version is a 4.x version that precedes the upgrade version.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes.
- No port in the fabric is in the diagnostic state.
- No zoning changes are being made in the fabric.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.

Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, SANsurfer Switch Manager sessions reconnect automatically. However, Telnet sessions must be restarted manually.

4.3.1
Using SANsurfer Switch Manager to Install Firmware

To install firmware using SANsurfer Switch Manager, do the following:

1. Select a switch in the topology display and double-click to open the Faceplate display. Open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload window, click the **Select** button to browse and select the firmware file to be uploaded.
3. Click the **Start** button to begin the loading process.

4.3.2
Using the CLI to Install Firmware

To install firmware using the CLI when a File Transfer Protocol (FTP) server is present on the management workstation, use the Firmware Install command. Refer to the "Firmware Install Command" on page B-23 for more information.

1. Enter the following command to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware. If possible, a non-disruptive activation will be performed.

```
SANbox2 (admin) #> firmware install

Warning: Installing new firmware requires a switch reset. A
stable farbic is required to successfully activate the
firmware on a switch without disrupting traffic. Therefore,
before continuing with this action, ensure there are no
administrative changes in progressanywhere in the fabric.

Continuing with this action will terminate all management
sessions, including any Telnet sessions. When the firmware
activation is complete, you may log in to the switch again.

Do you want to continue? [y/n]: y

Press 'q' and the ENTER key to abort this command.
```

2. Enter your account name on the remote host and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

```
User Account : johndoe
IP Address : 10.20.20.200
Source Filename : 4.0.2.00.04_x86
```

3. When prompted to install the new firmware, enter Yes to continue or No to cancel. If possible, a non-disruptive activation will be performed. This is the last opportunity to cancel.

```
About to install image. Do you want to continue? [y/n] y
Connected to 10.20.20.200 (10.20.20.200).
220 localhost.localdomain FTP server (Version
wu-2.6.1-18) ready.
```

4. Enter the password for your account name. The firmware will now be downloaded from the remote host to the switch, installed, and activated.

```
331 Password required for johndoe.
Password:******
230 User johndoe logged in.
```

4.4 Powering Down a Switch

Simply unplugging the switch from the power source does not allow the switch to complete executing tasks and could lead to flash memory corruption. For this reason, open a Telnet session and use the Shutdown command to initiate an orderly shut down, then power down the switch. Refer to the “Shutdown Command” on page B-114.

Notes

Section 5

Diagnostics/Troubleshooting

Diagnostic information about the switch is available through the chassis LEDs and the port LEDs. Diagnostic information is also available through the SANsurfer Switch Manager and CLI event logs and error displays. This section describes two types of diagnostics: Power On Self Test (POST) and chassis. POST diagnostics describe the Heartbeat LED and the port Logged-In LED indications. Chassis diagnostics cover power supply and fan diagnostics as well as over temperature conditions. This section also describes how to use maintenance mode to recover a disabled switch.

5.1 POST Diagnostics

The switch performs a series of Power On Self Tests (POST) as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in PROM and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the ASIC

During the POST, the switch logs any errors encountered. Some POST errors are critical, others are not. The switch uses the Heartbeat LED and the Logged-In LED to indicate switch and port status. A critical error disables the switch so that it will not operate. A non-critical error allows the switch to operate, but disables the ports that have errors. Whether the problem is critical or not, contact your authorized maintenance provider.

If there are no errors, the Heartbeat LED blinks at a steady rate of once per second. If a critical error occurs, the Heartbeat LED will show an error blink pattern. If there are non-critical errors, the switch disables the failed ports and flashes the associated Logged-In LEDs. Refer to “Heartbeat LED Blink Patterns” on page 5-2 for more information about Heartbeat LED blink patterns.

5.1.1
Heartbeat LED Blink Patterns

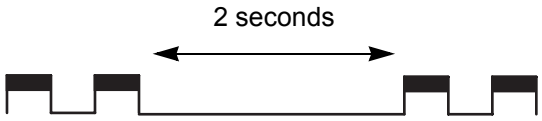
The Heartbeat LED indicates the operational status of the switch. When the POST completes with no errors, the Heartbeat LED blinks at steady rate of once per second. When the switch is in maintenance mode, the Heartbeat LED illuminates continuously. Refer to “Recovering a Switch” on page 5-11 for more information about maintenance mode. All other blink patterns indicate critical errors.

The Heartbeat LED shows an error blink pattern for the following conditions:

- 2 blinks - Internal Firmware Failure Blink Pattern
- 3 blinks - System Error Blink Pattern
- 4 blinks - Configuration File System Error Blink Pattern

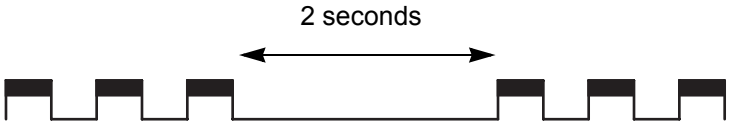
5.1.1.1
Internal Firmware Failure Blink Pattern

An internal firmware failure blink pattern is 2 blinks followed by a two second pause. The 2-blink error pattern indicates that the firmware has failed, and that the switch must be reset. Momentarily press and release the Maintenance button to reset the switch.



5.1.1.2
System Error Blink Pattern

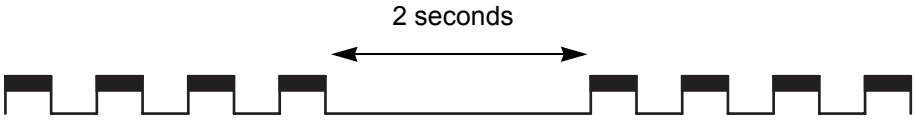
A system error blink pattern is 3 blinks followed by a two second pause. The 3-blink error pattern indicates that a POST failure or a system error has left the switch inoperable. If a system error occurs, contact your authorized maintenance provider. Momentarily press and release the Maintenance button to reset the switch.



5.1.1.3

Configuration File System Error Blink Pattern

A configuration file system error blink pattern is 4 blinks followed by a two second pause. The 4-blink error pattern indicates that a configuration file system error has occurred, and that the configuration file must be recreated. Refer to “Recovering a Switch” on page 5-11 for more information.



To recreate the configuration file, do the following:

CAUTION! Recreating the configuration file deletes all configuration settings.

1. Open a Telnet session and use the Shutdown command to close activity on the switch, then power down the switch. Refer to the “Shutdown Command” on page B-114.
2. Place the switch in maintenance mode. Press and hold the Maintenance button for 2–4 seconds. Refer to “Recovering a Switch” on page 5-11 for more information about placing the switch in maintenance mode.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

   ```
   telnet 10.0.0.1
   ```

4. Enter the account name (prom) and password (prom),

   ```
   Switch login: prom
   Password:xxxx
   [username@host:Itasca]% telnet 10.0.0.1
   Trying 10.0.0.1...
   Connected to 10.0.0.1.
   Escape character is '^]'.
   ```

5. The following menu is displayed. Enter "6" (Remake Filesystem) and press the Enter key to recreate the configuration file.

   ```
   0)  Exit
   1)  Image Unpack
   2)  Reset Network Config
   3)  Reset User Accounts to Default
   4)  Copy Log Files
   5)  Remove Switch Config
   6)  Remake Filesystem
   7)  Reset Switch
   Option: 6
   ```

6. When the recreate process is complete, select option 7 to reset the switch and exit maintenance mode.
7. If a previously saved configuration file is available for the switch, do the following to restore the configuration file.
   a. Establish communications with the switch using the File Transfer Protocol (FTP) by entering the following on the command line:

      ```
      >ftp 10.0.0.1
      ```

   b. Enter the following account name and password:

      ```
      user:images
      password:images
      ```

   c. Activate binary mode and copy the configuration file from the workstation to the switch. The configuration file must be named "configdata".

      ```
      ftp>bin
      ftp>put configdata
      ```

   d. Close the FTP session.

      ```
      ftp>quit
      ```

   e. Establish communications with the switch using Telnet. Enter one of the following on the command line:

      `telnet` *`xxx.xxx.xxx.xxx`*

      or

      `telnet` *`switchname`*

      where *xxx.xxx.xxx.xxx* is the switch IP address and *switchname* is the switch name associated with the IP address.

   f. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).

   g. Open an admin session to acquire the necessary authority.

      ```
      SANbox2 $>admin start
      ```

   h. Restore the configuration file. When the restore is complete, the switch will reset.

      ```
      SANbox2 (admin) $>config restore
      ```

5.1.2

Logged-In LED Indications

Port diagnostics are indicated by the Logged-In LED for each port as shown in Figure 5-1.

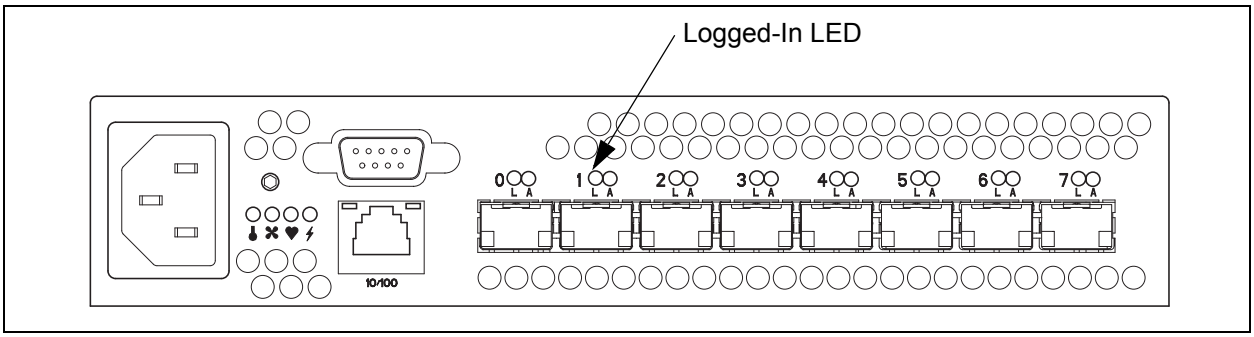


Figure 5-1. Logged-In LED

The Logged-In LED has three indications:

- Continuous illumination: A device is logged in to the port.
- Flashing once per second: A device is logging in to the port.
- Flashing twice per second: The port is down, offline, or an error has occurred.

If a Logged-In LED shows an error indication, review the event browser for alarm messages regarding the affected port. You can also inspect the event log using the Show Alarm command. Pertinent alarm messages will point to one or more of the following conditions:

- E_Port isolation
- Excessive port errors

5.1.2.1

E_Port Isolation

A Logged-In LED error indication is often the result of E_Port isolation. An isolated E_Port is indicated by a red link in the SANsurfer Switch Manager topology display. E_Port isolation can be caused by the following:

- Security failure
- FL_Port is connected to another switch
- Conflicting domain IDs
- Conflicting timeout values
- Conflicting zone membership between active zone sets

Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about how to change domain IDs, timeout values, and edit zoning. Review the event browser and do the following to diagnose and correct an isolated E_Port:

1. Does the event browser show an invalide attach alarm for the affected port?
   - Yes - Review the ISL group in the active security set to ensure that the membership includes the necessary ports and that the secrets on all switches are correct.
   - No - Continue.
2. Does the event browser show a repeating alarm about an unsupported E_Port command on the affected port?
   - Yes - The port is configured as an FL_Port and connected to another switch. Correct the port connection or the port type.
   - No - Continue.
3. Display the fabric domain IDs using the Show Domains command or the Switch data tab in the SANsurfer Switch Manager topology display. Are all domain IDs in the fabric unique?
   - Yes - Continue.
   - No - Correct the domain IDs on the offending switches using the Set Config Switch command or the SANsurfer Switch Manager Switch Properties window. Reset the port. If the condition remains, continue.
4. Compare the RA_TOV and ED_TOV timeout values for all switches in the fabric using the Show Config Switch command or the Switch data tab of the SANsurfer Switch Manager topology display. Are the timeout values the same?
   - Yes - Continue.
   - No - Correct the timeout values on the offending switches using the Set Config Switch command or the SANsurfer Switch Manager Switch Properties dialog. Reset the port. If the condition remains, continue.

5. Display the active zone set on each switch using the Zoning Active command or the Active Zoneset tab of the SANsurfer Switch Manager topology display. Compare the zone membership between the two active zone sets. Are they the same?
   - Yes - Contact your authorized maintenance provider.
   - No - Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same. Reset the port. If the condition remains, contact your authorized maintenance provider.

     Note: This can be caused by merging two fabrics whose active zone sets have two zones with the same name, but different membership.

5.1.2.2

Excessive Port Errors

The switch monitors a set of port errors and generates alarms based on user-defined sample windows and thresholds. These port errors include the following:

- CRC errors
- Decode errors
- ISL connection count
- Login errors
- Logout errors
- Loss-of-signal errors

Port threshold alarm monitoring is disabled by default. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about managing port threshold alarms.

If the count for any of these errors exceeds the rising trigger for three consecutive sample windows, the switch generates an alarm and disables the affected port, changing its operational state to "down". Port errors can be caused by the following:

- Triggers are too low or the sample window is too small
- Faulty Fibre Channel port cable
- Faulty SFP
- Faulty port
- Fault device or HBA

Review the event browser to determine if excessive port errors are responsible for disabling the port. Look for a message that mentions one of the monitored error types indicating that the port has been disabled, then do the following:

1. Examine the alarm configuration for the associated error using the Show Config Threshold command or the SANsurfer Switch Manager application. Refer to the "Show Config Command" on page B-102. Refer to Table B-11 for a list of the alarm configuration defaults. Are the thresholds and sample window correct?
   - Yes - Continue
   - No - Correct the alarm configuration. If the condition remains, continue.
2. Reset the port, then perform an external port loopback test to validate the port and the SFP. Refer to the "Test Command" on page B-115 or the *SANbox2-8c/16 Switch Management User's Guide* for information about testing ports. Does the port pass the test?
   - Yes - Continue
   - No - Replace the SFP and repeat the test. If the port does not pass the test, contact your authorized maintenance provider. Otherwise continue.
3. Replace the Fibre Channel port cable. Is the problem corrected?
   - Yes - Complete.
   - No - Continue.
4. Inspect the device to which the affected port is connected and confirm that the device and its HBA are working properly. Make repairs and corrections as needed. If the condition remains, contact your authorized maintenance provider.

5.2 Chassis Diagnostics

Chassis diagnostics are indicated by the chassis LEDs as shown in Figure 5-2.

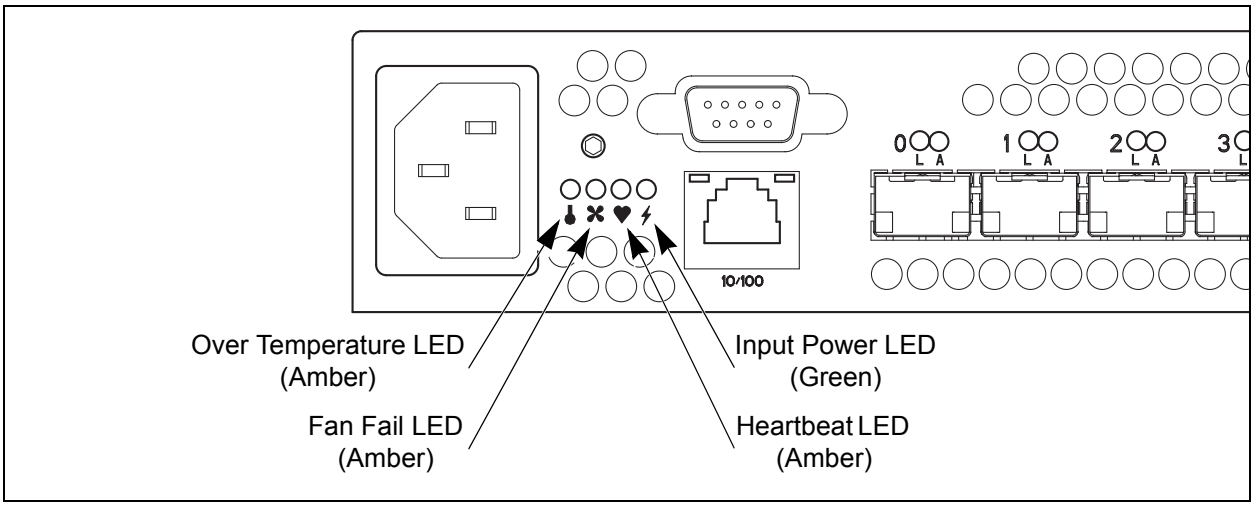


Figure 5-2. Chassis LEDs

The following conditions are described:

- Over Temperature LED is illuminated
- Input Power LED is extinguished
- Fan Fail LED is illuminated

5.2.1 Over Temperature LED is Illuminated

The Over Temperature LED illuminates to indicate that the switch logic circuitry is has exceeded the failure temperature threshold. The failure temperature threshold is 70° C. If the Over Temperature LED illuminates, do the following:

1. Inspect the chassis fan. Is the intake opening clear? Is the fan operating and producing air flow?
   - Yes - Continue.
   - No - Remove any debris from fan intake and exhaust if necessary. If the condition remains, continue.
2. Consider the ambient air temperature near the switch and clearance around the switch. Make necessary corrections. If the condition remains, contact your authorized maintenance provider.

5.2.2
Input Power LED Is Extinguished

The Input Power LED illuminates to indicate that the switch logic circuitry is receiving proper voltages. If the Input Power LED is extinguished, do the following:

1. Inspect the power cords and connectors. Is the cord unplugged? Is the cord or connector damaged?
   - Yes - Make necessary corrections or repairs. If the condition remains, continue.
   - No - Continue.
2. Inspect the AC power source. Is the power source delivering the proper voltage?
   - Yes - Continue
   - No - Make necessary repairs. If the condition remains, contact your authorized maintenance provider.

5.2.3
Fan Fail LED is Illuminated

The Fan Fail LED illuminates to indicate a malfunction with the chassis fan. If the Fan Fail LED illuminates, isolate the switch from the fabric, unplug the switch from the AC power source, and contact your authorized maintenance provider.

5.3
Recovering a Switch

A switch can become inoperable or unmanageable for the following reasons:

- Firmware becomes corrupt
- IP address is lost
- Switch configuration becomes corrupt
- Forgotten password

In these specific cases, you can recover the switch using maintenance mode. Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to do the following:

- Unpack a firmware image file
- Restore the network configuration parameters to the default values
- Remove all user accounts and restore the Admin account name password to the default.
- Copy the log file
- Restore factory defaults for all but user accounts and zoning
- Restore all switch configuration parameters to the factory default values
- Reset the switch

To recover a switch, do the following:

1. Place the switch in maintenance mode. Press and hold the Maintenance button with a pointed tool for 2–4 seconds. When the Input Power LED alone is illuminated, release the button.
2. Allow one minute for the switch to complete its tests. When the switch is in maintenance mode, the Input LED will be illuminated and the Heartbeat LED will illuminate continuously. All other chassis LEDs will be extinguished.
3. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.
4. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

```
Sanbox login: prom
Password:xxxx
[username@anteater:Itasca]% telnet 10.0.0.1
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
```

5. The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press the Enter key.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
Option:
```

These options and their use are described in the following subsections.

5.3.1 Maintenance – Exit

This option closes the current login session. To log in again, enter the maintenance mode account name and password (prom, prom). To return to normal operation, momentarily press and release the Maintenance button or power cycle the switch.

5.3.2 Maintenance – Image Unpack

This option unpacks and installs new firmware when the current firmware has become corrupt. Before using this option, you must load the new firmware image file onto the switch. The steps to install new firmware using this option are as follows:

1. Place the switch in maintenance mode. Refer to the procedure for maintenance mode in “Recovering a Switch” on page 5-11.
2. Use FTP to load a new firmware image file onto the switch. Refer to the “Image Command” on page B-36 for an example of how to load the image file using FTP. Close the FTP session.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

```
telnet 10.0.0.1
```

4. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

```
Sanbox login: prom
Password:xxxx
```

5. Select option 1 from the maintenance menu. When prompted for a file name prompt, enter the firmware image file name.

```
Image filename: filename
Unpacking 'filename', please wait...
Unpackage successful.
```

6. Select option 7 to reset the switch and exit maintenance mode.

5.3.3 Maintenance – Reset Network Config

This option resets the network properties to the factory default values and saves them on the switch. Refer to Table B-16 for the default network configuration values.

5.3.4 Maintenance – Reset User Accounts to Default

This option restores the password for the Admin account name to the default (password) and removes all other user accounts from the switch.

5.3.5 Maintenance – Copy Log Files

This option copies all log file buffers to a file on the switch named *logfile*. You can use FTP to download this file to the management workstation. You must download the logfile before resetting the switch.

5.3.6 Maintenance – Remove Switch Config

This option deletes all configurations from the switch except for the default configuration. This restores switch configuration parameters to the factory defaults except for user accounts and zoning. Refer to Table B-9 though Table B-16 for the factory default values.

5.3.7
Maintenance – Remake Filesystem

In the event of sudden loss of power, it is possible that the switch configuration may become corrupt. The file system on which the configuration is stored must be re-created. This option resets the switch to the factory default values including user accounts and zoning. Refer to Table B-9 though Table B-16 for the factory default values.

CAUTION! If you choose the **Remake Filesystem** option, you will lose all changes made to the fabric configuration that involve that switch, such as password and zoning changes. You must then restore the switch from an archived configuration or reconfigure the portions of the fabric that involve the switch.

5.3.8
Maintenance – Reset Switch

This option closes the Telnet session, exits maintenance mode and reboots the switch using the current switch configuration. All unpacked firmware image files that reside on the switch are deleted.

Appendix A
Specifications

This appendix contains the specifications for the SANbox2-8c Fibre Channel switch. Refer to Section 2 General Description for the location of all connections, switches, controls, and components.

A.1 Fabric Specifications

Fibre Channel Protocols	FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-AL Rev 4.5 FC-AL-2 Rev 7.0 FC-FLA FC-GS-3 FC-FG FC-Tape FC-VI FC-SW-2 Fibre Channel Element MIB RFC 2837 Fibre Alliance MIB Version 4.0
Fibre Channel Classes of Service ..	Classes 2 and 3
Modes of Operation	Fibre Channel Classes 2 and 3, connectionless
Port Types.....	F_Port FL_Port E_Port G_Port GL_Port
Port Characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel Ports	8 ports per chassis
Scalability.....	Maximum 239 switches depending on configuration
Maximum User Ports	> 475,000 ports depending on configuration

Buffer Credits	12 buffer credits per port
Media Type	Small Form Pluggable (SFP) optical transceivers. Hot swappable. 3.3 Volts.
Fabric Port Speed	1.0625 or 2.125-Gbps
Maximum Frame Size	2148 bytes (2112 byte payload)
System Processor	266 MHz Geode® processor
Fabric Latency (best case)	<0.4 µsec.
Fabric Point-to-Point Bandwidth	1.0625 or 2.125-Gbps, full duplex
Fabric Aggregate Bandwidth	16 Gb/s for a single switch

A.2 Maintainability

Diagnostics	Power On Self Test (POST) tests all functional components except SFP transceivers. Port tests include online, internal, and external tests.
User Interface	LED indicators

A.3 Fabric Management

Management Methods	SANsurfer Switch Manager Graphical User Interface Application Programming Interface Command Line Interface GS-3 Management Server SNMP FTP
Maintenance Connection	RS-232 connector; null modem F/F DB9 cable
Ethernet Connection	RJ-45 connector; 10/100 BASE-T cable
Switch Agent	Allows a network management station to obtain configuration values, traffic information, and failure data pertaining to the Fibre Channels using SNMP through the Ethernet interface.

A.4 Dimensions

Width	8.5” (216 mm), 19 inch rack mount
Height	1.75” (44 mm) (1U)
Depth	20.0” (508 mm)
Weight	8.5 lbs (3.86 Kg)

A.5 Electrical

Operating voltage	90 to 137 Vac; 47 to 63 Hz 180 to 264 Vac; 47 to 63 Hz
Power source loading	1.0 Amps maximum at 90 to 137 Vac 0.45 Amps maximum at 180 to 264 Vac
Heat Output (maximum)	70 watts
Circuit Protection	Internally fused

A.6 Environmental

Temperature
- Operating ..... 5 to 50°C (41 to 122°F)
- Non-operating ..... -40 to 65°C (-40 to 149°F)

Humidity
- Operating ..... 15% to 80%, non-condensing
- Non-operating ..... 25% to 90%, non-condensing

Altitude
- Operating ..... 0 to 3048m (0 to 10,000 feet)
- Non-operating ..... 0 to 15,240m (0 to 50,000 feet)

Vibration IEC 68-2
- Operating ..... 5-500 Hz, random, 0.21 G rms, 10 minutes
- Non-operating ..... 5-500 Hz, random, 2.09 G rms, 10 minutes

Shock IEC 68-2
- Operating ..... 4 g, 11ms, 20 repetitions
- Non-operating ..... 30g, 292 ips, 3 repetitions, 3 axis

Air flow ..... Front-to-back or back-to-front, by model

A.7
Regulatory Certifications

Safety Standards	UL1950, CSA 22.2 No. 950, EN60950
Emissions Standards	FCC Part 15B Class A ICES-03 Issue 3 VCCI Class A ITE BSMI Class A CISPR 22, Class A EN 55022, Class A
Voltage Fluctuations	EN 61000-3-3
Harmonics.....	EN 61000-3-2
Immunity	EN 55024:1998
Marking	FCC Part 15,UL (United States), cUL (Canada), TUV, VCCI, BSMI, CE
SANmark®	SCD 3001, 3002, 3010, 3020

Notes

Appendix B

Command Line Interface

The command line interface (CLI) enables you to perform a variety of fabric and switch management tasks through an Ethernet or a serial port connection. This section describes the following:

- Logging On to a Switch
- User Accounts
- Working with Switch Configurations
- Commands

B.1 Logging On to a Switch

To log on to a switch using Telnet, open a command line window on the workstation and enter the Telnet command followed by the switch IP address:

```
# telnet ip_address
```

A Telnet window opens prompting you for a login. Enter an account name and password.

To log on to a switch through the serial port, configure the workstation port with the following settings:

- 9600 baud
- 8-bit character
- 1 stop bit
- No parity

Enter an account name and password when prompted.

B.2 User Accounts

Switches come from the factory with the following user account already defined:

Account name: admin
Password: password
Authority: Admin

This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account.

- Refer to “Commands” on page B-6 for information about authority levels.
- Refer to the “User Command” on page B-119 for information about creating user accounts.
- Refer to “Passwd Command” on page B-40 for information about changing passwords.

Note: A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for SANsurfer Switch Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins. Additional logins will be refused.

B.3 Working with Switch Configurations

Successful management of switches and fabrics with the command line interface depends on the effective use of switch configurations. Modifying configurations, backing up configurations, and restoring configurations are key switch management tasks.

B.3.1
Modifying a Configuration

A switch supports up to 10 configurations including the default configuration. Each switch configuration contains switch, port, port threshold alarm, and zoning configuration components. The Show Switch command displays the name of the active configuration. A configuration name can have up to 31 characters excluding the pound symbol (#), semicolon (;), and comma (,). By editing the latest configuration and saving the results under a new name, you can create a history of configuration changes. Use the Config List command to display the configurations stored on the switch

```
SANbox2 #> config list
  Current list of configurations
  ------------------------------
  default
  config_10132003
```

To modify a switch configuration you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through Telnet or SANsurfer Switch Manager. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name the active configuration is assumed. The Config Edit session provides access to the Set Config commands with which you make modifications to the port, switch, port threshold alarm, or zoning configuration components as shown:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit default
   The config named default is being edited.
SANbox2 (admin-config)#> set config port . . .
SANbox2 (admin-config)#> set config switch . . .
SANbox2 (admin-config)#> set config threshold . . .
SANbox2 (admin-config)#> set config zoning . . .
```

The Config Save command saves the changes you made during the Config Edit session. In this case, changes to the configuration named *Default* are being saved to a new configuration named *config_10132003*. However, the new configuration does not take effect until you activate it with the Config Activate command:

```
SANbox2 (admin-config)#> config save config_10132003
SANbox2 (admin)#> config activate config_10132003
SANbox2 (admin)#> admin end
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

B.3.2
Backing up and Restoring Switch Configurations

Backing up and restoring a configuration is useful to protect your work or for use as a template in configuring other switches. The Config Backup command creates a file on the switch, named *configdata*. This file can be used to restore a switch configuration only from the command line interface; it cannot be used to restore a switch using SANsurfer Switch Manager.

```
SANbox2  #> admin start
SANbox2 (admin) #> config backup
```

The *configdata* file contains all of the switch configuration information including the following:

- All named switch configurations including the default configuration. This includes port, switch, port threshold alarm, and zoning configuration components.
- All SNMP and network information defined with the Set Setup command.
- The zoning database included all zone sets, zones, and aliases

You use FTP to download the *configdata* file to your workstation for safe keeping and to upload the file back to the switch for the restore function. To download the configdata file, open an FTP session on the switch and login with the account name *images* and password *images*. Transfer the file in binary mode with the Get command as shown:

```
>ftp ip_address
user:images
password: images

ftp>bin
ftp>get configdata
    xxxxx bytes sent in xx secs.
ftp>quit
```

You should rename the *configdata* file on your workstation with the switch name and date, *config_switch_169_10112003*, for example.

The restore operation begins with FTP to upload the configuration file from the workstation to the switch, then finishes with a Telnet session and the Config Restore command. To upload the configuration file, *config_switch_169_10112003* in this case, open and FTP session with account name *images* and password *images*. Transfer the file in binary mode with the Put command as shown:

```
ftp ip_address
user:images
password: images
ftp> bin
ftp> put config_switch_169_10112003 configdata
  Local file config_switch_169_10112003
  Remote file configdata
ftp>quit
```

The restore process replaces all configuration information on the switch and afterwards the switch is automatically reset. If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the “Set Setup Command” on page B-77. To restore the switch, open a Telnet session, then enter the Config Restore command from within an Admin session as shown:

```
SANbox2  #> admin start
SANbox2 (admin) #> config restore
  The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
```

B.4 Commands

The command syntax is as follows:

command
keyword
keyword *[value]*
keyword [value1] [value2]

The **Command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case insensitive.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value].*
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example the Delete keyword can be abbreviated Del.

The command-line completion feature makes entering and repeating commands easier. Table B-1 describes the command-line completion keystrokes.

Table B-1. Command-Line Completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press the Tab key again to display all possibilities.
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves the cursor to the beginning of the command line
Control-E	Moves the cursor to the end of the command line.

The command set performs monitoring and configuration tasks. Commands related to monitoring tasks are available to all account names. Commands related to configuration tasks are available only within an admin session. An account must have Admin authority to enter the Admin Start command, which opens an admin session. Refer to the “Admin Command” on page B-8.

The commands and their page numbers are listed in Table B-2.

Table B-2. Commands Listed by Authority Level

Monitoring Commands		Configuration Command	
Help	(B-33)	Admin	(B-8)
History	(B-34)	**Admin Session Commands**	
Ping	(B-41)	Alias[1]	(B-9)
Ps	(B-42)	CIM[1]	(B-11)
Quit	(B-43)	CIMListener	(B-12)
Show	(B-87)	CIMSubscription	(B-14)
Show Config	(B-102)	Config[1]	(B-16)
Show Log	(B-105)	Create	(B-19)
Show Perf	(B-108)	Date[1]	(B-22)
Show Setup	(B-110)	Firmware Install	(B-23)
Uptime	(B-118)	Group[1]	(B-24)
Whoami	(B-122)	Hardreset	(B-32)
		Hotreset	(B-35)
		Image	(B-36)
		Lip	(B-39)
		Passwd	(B-40)
		Reset	(B-44)
		Security	(B-52)
		Securityset[1]	(B-56)
		Set[1]	(B-58)
		Set Config	(B-60)
		Set Log	(B-71)
		Set Port[1]	(B-75)
		Set Setup	(B-77)
		Shutdown	(B-114)
		Test	(B-115)
		User[1] [2]	(B-119)
		Zone[1]	(B-123)
		Zoneset[1]	(B-127)
		Zoning[1]	(B-129)

[1]Some keywords do not require an Admin session.

[2] Some keywords can be executed only by the Admin account name.

Admin Command

Opens and closes an Admin session. The Admin session provides commands that change the fabric and switch configurations. Only one Admin session can be open on the switch at any time. An inactive Admin session will time out after a period of time which can be changed using the Set Setup System command. Refer to the "Set Setup Command" on page B-77.

Authority Admin

Syntax

admin
start (or begin)
end (or stop)
cancel

Keywords

start (or begin)
Opens the admin session.

end (or stop)
Closes the admin session. The Hardreset, Hotreset, Logout, Shutdown, and Reset Switch commands will also end an admin session.

cancel
Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an admin session does not release the session. In this case, you must either wait for the admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
SANbox2 #> admin start

SANbox2 (admin) #>

.
.
.

SANbox2 (admin) #> admin end
SANbox2 #>
```

Alias Command

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session for all keywords except List and Members

Syntax **alias**

add [alias] [member_list]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [member_list]
rename [alias_old] [alias_new]

Keywords **add [alias] [member_list]**
Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]
Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]
Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]
Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all aliases. This keyword does not require an admin session.

members [alias]
Displays all members of the alias given by [alias]. This keyword does not require an admin session.

remove [alias] [member_list]
Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]
Renames the alias given by [alias_old] to the alias given by [alias_new].

CIM Command

Manages CIM listener and subscription configurations on the switch. Refer to the "CIMListener Command" on page B-12 for information about creating and modifying CIM listeners. Refer to the "CIMSubscription Command" on page B-14 for information about creating and modifying CIM subscriptions.

Authority Admin session

Syntax **cim**
- cancel
- clear
- edit
- limits
- save

Keywords

cancel
Terminates the current CIM edit session without saving changes that were made.

clear
Clears all CIM listener and subscription configurations from the switch.

edit
Opens a CIM edit session.

limits
Displays the maximum allowed number of CIM listeners, subscriptions, and subscriptions per listener. This keyword does not require an Admin session nor a CIM edit session.

save
Saves all changes made during the current CIM edit session.

Examples The following is an example of the CIM Edit command:

```
SANbox2 (admin) #> cim edit
SANbox2 (admin-cim) #> cimlistener create CIM_listener_1
.
.
.
SANbox2 (admin-cim) #> cim save
```

The following is an example of the CIM Limits command:

```
SANbox2 #> cim limits

  Cim Attribute                Maximum
  -------------                -------
  MaxListeners                 32
  MaxSubscriptions             50
  MaxSubscriptionsPerListener  6
```

CIMListener Command

Configures CIM indication service listeners and adds subscriptions to listeners. Refer to the "CIMSubscription Command" on page B-14 for information about configuring subscriptions.

Authority Admin session and a CIM Edit session. Refer to the "CIM Command" on page B-11 for information about opening a CIM edit session.

Syntax

cimlistener
add [listener_name] [subscription_list]
create [listener_name]
delete [listener_name]
edit [listener_name]

Keywords

add [listener_name] [subscription_list]
Adds the set of subscriptions given by [subscription_list] to the listener given by [listener_name]. Use a <space> to delimit subscription names in [subscription_list].

create [listener_name]
Prompts you in a line-by-line fashion to create a CIM listener with the name given by [listener_name]. [listener_name] can have up to 32 characters: 0-9, A-Z, a-z, _, $, ^, and -. The CIM listener configuration parameters are described in Table B-3.

Table B-3. CIM Listener Configuration Parameters

Parameter	Description
Name	Listener name
Type	Listener type: ■ Permanent – Send indications to the CIM client whether a connection can be established or not. This is the default. ■ Transient – Sends indications to the CIM client, but ceases if a connection cannot be established after 60 minutes.
URL	IP address of the CIM client and the port number to which to send indications. The default is 10.0.0.1:5000.

delete [listener_name]
Deletes the listener given by [listener_name] from the CIM database.

edit [listener_name]
Opens an editing session in which you can modify the CIM listener given by [listener_name]. Refer to Table B-3 for a description of the CIM listener configuration parameters.

Examples

The following is an example of the CIMListener Create command:

```
SB5602-91.54 (admin-cim) #> cimlistener create listener_1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Name  listener_1
  Type  (2=Permanent, 3=Transient)   [Permanent    ]
  URL   (IP address:port format)     [10.0.0.1:5000]

  Finished configuring attributes.
  This configuration must be saved with the cim save command
  before it can take effect, or to discard this configuration
  use the cim cancel command.
```

CIMSubscription Command

Creates, edits, or removes CIM subscriptions.

Authority Admin session and a CIM Edit session. Refer to the "CIM Command" on page B-11 for information about opening a CIM edit session.

Syntax

cimsubscription
create [subscription_name]
delete [subscription_name]
edit [subscription_name]

Keywords

create [subscription_name]
Prompts you in a line-by-line fashion to create a CIM subscription with the name given by [subscription_name]. [subscription_name] can have up to 32 characters: 0-9, A-Z, a-z, _, $, ^, and -. Table B-4 describes the CIM subscription configuration parameters.

Table B-4. CIM Subscription Configuration Parameters

Parameter	Description
Name	Subscription name.
FilterID	Event type for which the switch monitors and sends an indication to the CIM client. The event types are as follows: ■ CreateComputerSystem – A switch is added to the fabric. This is the default. ■ ModifyComputerSystem – A switch state change. ■ DeleteComputerSystem – A switch is removed from the fabric. ■ CreateFCPort – Not supported. ■ ModifyFCPort – A Fibre Channel port state change. ■ DeleteFCPort – Not supported.
EnabledState	Enable (True) or disable (False) the subscription. The default is True.
Duration	Subscription life span in seconds. The subscription life span begins when the subscription is created. Expired subscriptions do not send indications to the CIM client though they remain in the CIM database. Values can be 1–720000. 0 indicates indefinite, which is the default.

delete [subscription_name]
Deletes the subscription given by [subscription_name] from the CIM database.

edit [subscription_name]
Opens an editing session in which you can modify the CIM subscription given by [subscription_name]. Refer to Table B-4 for a description of the CIM subscription configuration parameters.

Examples

The following is an example of the CIMSubscription Create command:

```
SANbox2 (admin-cim) #> cimsubscription create subscription_1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

     FilterID values:  1 = Create:ComputerSystem
                       2 = Modify:ComputerSystem
                       3 = Delete:ComputerSystem
                       4 = Create:FCPort
                       5 = Modify:FCPort
                       6 = Delete:FCPort

  Name          subscription_1
  FilterID      (see allowed options above)              [Create:ComputerSystem]
  EnabledState  (True / False)                           [True                 ]
  Duration      (decimal value, 0-720000 secs, 0=forever) [0                    ]

  Finished configuring attributes.
  This configuration must be saved with the cim save command
  before it can take effect, or to discard this configuration
  use the cim cancel command.
```

Config Command

Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, refer to the “Set Config Command” on page B-60.

Authority Admin session for all keywords except List

Syntax

config
activate *[config_name]*
backup
cancel
copy [config_source] [config_destination]
delete [config_name]
edit *[config_name]*
list
restore
save *[config_name]*

Keywords

activate *[config_name]*
Activates the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used. Only one configuration can be active at a time.

backup
Creates a file named *configdata*, which contains the system configuration information. To download this file, open an FTP session, log in with account name/password of “images” for both, and type “get configdata”. Refer to “Backing up and Restoring Switch Configurations” on page B-4.

cancel
Terminates the current configuration edit session without saving changes that were made.

copy [config_source] [config_destination]
Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

delete [config_name]
Deletes the configuration given by [config_name] from the switch. You cannot delete the default configuration (Default Config) nor the active configuration.

edit *[config_name]*
Opens an edit session for the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used.

list
Displays a list of all available configurations on the switch. This keyword does not require an admin session.

restore
Restores configuration settings to an out-of-band switch from a backup file named *configdata*, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, then enter the Config Restore command. After the restore is complete, the switch automatically resets. Refer to "Backing up and Restoring Switch Configurations" on page B-4.

Note:
- If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the "Set Setup Command" on page B-77.
- Configuration archive files created with the SANsurfer Switch Manager Archive function are not compatible with the Config Restore command.

save *[config_name]*
Saves changes made during a configuration edit session in the configuration given by [config_name]. If you omit [config_name], the value for [config_name] you chose for the most recent Config Edit command is used. [config_name] can be up to 31 characters excluding #, semicolon (;), and comma (,). The switch supports up to 10 configurations including the default configuration.

Notes

If you edit the active configuration, changes will be held in suspense until you reactivate the configuration or activate another configuration.

Examples

The following shows an example of how to open and close a Config Edit session:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
   The config named default is being edited.
.
.
SANbox2 (admin-config) #> config cancel
  Configuration mode will be canceled. Please confirm (y/n): [n] y
SANbox2 (admin) #> admin end
```

The following is an example of how to create a backup file (configdata) and download the file to the workstation.

```
SANbox2 #> admin start
SANbox2 (admin) #> config backup
SANbox2 (admin) #> admin end
SANbox2 #> exit

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> quit
```

The following is an example of how to upload a configuration backup file (configdata) from the workstation to the switch, and then restore the configuration.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

SANbox2 #> admin start


SANbox2 (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
  Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is being
restored -  this could take several minutes !]
  Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be reset in
3 seconds due to a config restore]
SANbox2 (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being reset]
Good bye.
```

Create Command

Creates support files for troubleshooting switch problems, and certificates for secure communications for SANsurfer Switch Manager.

Authority Admin session

Syntax

create
certificate
support

Keywords

certificate

Creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as SANsurfer Switch Manager. The certificate is valid 24 hours before the certificate creation date and expires 365 days after the creation date. Should the current certificate become invalid, use the Create Certificate command to create a new one.

Note: To insure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. Refer to the following:

- "Date Command" on page B-22 for information about setting the time and date
- "Set Command" on page B-58 (Timezone keyword) for information about setting the time zone on the switch and workstation
- "Set Setup Command" on page B-77 (System keyword) for information about enabling the Network Time Protocol for synchronizing the time and date on the switch and workstation from an NTP server.

support

Assembles all log files and switch memory data into a core dump file (dump_support.tgz) on the switch. If your workstation has an FTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP to download the support file from the switch to your workstation. The support file is useful to technical support personnel for troubleshooting switch problems. Use this command when directed by your authorized maintenance provider.

Examples The following is an example of the Create Support command when an FTP server is available on the workstation:

```
SANbox2 (admin) #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): y
Enter IP Address of remote computer: 10.20.33.130
Login name: johndoe
Enter remote directory name: bin/support
```

```
Would you like to continue downloading support file? (y/n) [n]: y

Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.

Password:  xxxxxxx


230 User johndoe logged in.
cd bin/support
250 CWD command successful.

lcd /itasca/conf/images

Local directory now /itasca/conf/images

bin

200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

The following is an example of the Create Support command and how to download the support file to your workstation. When prompted to send the support file to another machine, decline, then close the Telnet session. Open an FTP session on the switch and log in with the account name *images* and password *images*. Transfer the dump_support.tgz file in binary mode with the Get command.

```
SANbox2 (admin) #> create support

Log Msg:[Creating the support file - this will take several seconds]

FTP the dump support file to another machine? (y/n): n


SANbox2 (admin) #> quit

>ftp switch_ip_address

user:     images

password: images


ftp>bin

ftp>get dump_support.tgz

    xxxxx bytes sent in xx secs.

ftp>quit
```

The following is an example of the Create Certificate command:

```
SANbox2 (admin) #> create certificate
  The current date and time is day mon date hh:mm:ss UTC yyyy.
  This is the time used to stamp onto the certificate.
  Is the date and time correct? (y/n): [n] y
  Certificate generation successful.
```

Date Command

This command displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority Admin session except to display the date.

Syntax **date**
[MMDDhhmmCCYY]

Keywords ***[MMDDhhmmCCYY]***
Specifies the date – this requires an admin session. If you omit [MMDDhhmmCCYY], the current date is displayed which does not require an admin session.

Notes Network Time Protocol (NTP) must be disabled to set the time with the Date command. Refer to the "Set Setup Command" on page B-77, System keyword, for information about NTP.

When setting the date and time on a switch that is enabled for SSL connections, the switch time must be within 24 hours of the workstation time. Otherwise, the connection will fail.

Examples The following is an example of the Date command:

```
SANbox2 #> date
  Mon Apr 07 07:51:24 2003
```

Firmware Install Command

Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch (without a power-on self test) to activate the firmware. If possible, a non-disruptive activation is performed. The command prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

Authority Admin

Syntax **firmware install**

Examples The following is an example of the Firmware Install command:

```
SANbox2 (admin) #> firmware install
 Warning: Installing new firmware requires a switch reset.
 A stable farbic is required to successfully activate the firmware on a
 switch without disrupting traffic. Therefore, before continuing with
 this action, ensure there are no administrative changes in progress
 anywhere in the fabric.
 Continuing with this action will terminate all management sessions,
 including any Telnet sessions. When the firmware activation is complete,
 you may log in to the switch again.

 Do you want to continue? [y/n]: y
    Press 'q' and the ENTER key to abort this command.
  User Account    : johndoe
  IP Address      : 10.20.33.130
  Source Filename : 5.0.00.11_x86

  About to install image.  Do you want to continue? [y/n] y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Group Command

Creates groups, manages membership within the group, and manages the membership of groups in security sets.

Authority Admin session and a Security Edit session. Refer to the “Security Command” on page B-52 for information about starting a Security Edit session. The List, Members, Securitysets, and Type keywords are available without an Admin session.

Syntax **group**

add [group]
copy
create [group] *[type]*
delete [group]
edit [group] [member]
list
members [group]
remove [group] [member_list]
rename [group_old] [group_new]
securitysets [group]
type [group]

Keywords **add [group]**

Initiates an editing session in which to specify a group member and its attributes for the existing group given by [group]. ISL, Port, and MS member attributes are described in Table B-5, Table B-6, and Table B-7 respectively. The group name and group type attributes are read-only fields common to all three tables.

Table B-5. ISL Group Member Attributes

Attribute	Description
Member	Worldwide name of the switch that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the ISL member. The hash functions are MD5 or SHA-1. If the ISL member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the ISL group member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the ISL group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the ISL group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Binding	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the “Set Config Command” on page B-60. 0 (zero) specifies no binding.

Table B-6. Port Group Member Attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the Port group member. The hash functions are MD5 or SHA-1. If the Port group member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the Port group member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the Port group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the Port group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

Table B-7. MS Group Member Attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch.
CTAuthentication	Common Transport (CT) authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Hash	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Secret	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

copy [group_source] [group_destination]
Creates a new group named [group_destination] and copies the membership into it from the group given by [group_source].

create [group] ***[type]***
Creates a group with the name given by [group] with the type given by [type]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. [type] can be one of the following:

ISL
Configures security for attachments to other switches.

Port
Configures security for attachments to N_Port devices.

MS
Configures security for attachments to N_Port devices that are issuing management server commands.

edit [group] [member]
Initiates an editing session in which to change the attributes of a worldwide name given by [member] in a group given by [group]. Member attributes that can be changed are described in Table B-8:

Table B-8. Group Member Attributes

Attribute	Description
Authentication (ISL and Port Groups)	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP).
CTAuthentication (MS Groups)	CT authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Primary Hash (ISL and Port Groups)	The preferred hash function to use to decipher the encrypted Primary Secret sent by the member. The hash functions are MD5 or SHA-1. If the member does not support the Primary Hash, the switch will use the Secondary Hash.
Hash (MS Groups)	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Primary Secret (ISL and Port Groups)	Hexadecimal string that is encrypted by the Primary Hash for authentication with the member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash (ISL and Port Groups)	Hash function to use to decipher the encrypted Secondary Secret sent by the group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret (ISL and Port Groups)	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

Table B-8. Group Member Attributes (Continued)

Attribute	Description
Secret (MS Groups)	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Binding (ISL Groups)	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the "Set Config Command" on page B-60. 0 (zero) specifies no binding.

list
Displays a list of all groups and the security sets of which they are members. This keyword is available without an Admin session.

members [group]
Displays all members of the group given by [group]. This keyword is available without an Admin session.

remove [group] [member_list]
Remove the port/device worldwide name given by [member] from the group given by [group]. Use a <space> to delimit multiple member names in [member_list]

rename [group_old] [group_new]
Renames the group given by [group_old] to the group given by [group_new].

securitysets [group]
Displays the list of security sets of which the group given by [group] is a member. This keyword is available without an Admin session.

type [group]
Displays the group type for the group given by [group]. This keyword is available without an Admin session.

Notes

Refer to the "Securityset Command" on page B-56 for information about managing groups in security sets.

Examples

The following is an example of the Group Add command:

```
SANbox2 (admin-security) #> group add Group_1
  A list of attributes with formatting and default values will follow
  Enter a new value or simply press the ENTER key to accept the current value
  with exception of the Group Member WWN field which is mandatory.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name       Group_1
  Group Type       ISL
  Member          (WWN)                          [00:00:00:00:00:00:00:00]
  Authentication  (None / Chap)                  [None                    ]
  PrimaryHash     (MD5 / SHA-1)                  [MD5                     ]
  PrimarySecret   (32 hex or 16 ASCII char value)[                        ]
  SecondaryHash   (MD5 / SHA-1 / None)           [None                    ]
  SecondarySecret (40 hex or 20 ASCII char value)[                        ]
  Binding         (domain ID 1-239, 0=None)      [0                       ]


  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group Edit command:

```
SANbox2 (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name        g1
  Group Type        ISL
  Group Member      10:00:00:c0:dd:00:90:a3
  Authentication    (None / Chap)                  [None]  chap
  PrimaryHash       (MD5 / SHA-1)                  [MD5 ]  sha-1
  PrimarySecret     (40 hex or 20 ASCII char value)[    ]  12345678901234567890
  SecondaryHash     (MD5 / SHA-1 / None)           [None]  md5
  SecondarySecret   (32 hex or 16 ASCII char value)[    ]  1234567890123456
  Binding           (domain ID 1-239, 0=None)      [3   ]


  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group List command:

```
SANbox2 #> group list
  Group       SecuritySet
  -----       -----------
  group1 (ISL)
              alpha
  group2 (Port)
              alpha
```

The following is an example of the Group Members command:

```
SANbox2 #> group members group1
  Current list of members for Group: group1
  ---------------------------------
  10:00:00:c0:dd:00:71:ed
  10:00:00:c0:dd:00:72:45
  10:00:00:c0:dd:00:90:ef
  10:00:00:c0:dd:00:b8:b7
```

Hardreset Command

Resets the switch and performs a power-on self test. This reset disrupts traffic, activates the pending firmware, and clears the alarm log. To save the alarm log before resetting, refer to the “Set Log Command” on page B-71.

Authority Admin session

Syntax **hardreset**

Notes To reset the switch without a power-on self test, refer to the “Reset Command” on page B-44.

To reset the switch without disrupting traffic, refer to the “Hotreset Command” on page B-35.

Help Command

Displays a brief description of the specified command, its keywords, and usage.

Authority None

Syntax **help *[command] [keyword]***

Keywords ***[command]***
Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands.

[keyword]
Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all
Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Config command:

```
SANbox2 #> help config
config CONFIG_OPTIONS
The config command operates on configurations.

  Usage: config   { activate | backup   | cancel   | copy     | delete   |
                    edit     | list     | restore  | save }
```

The following is an example of the Help Config Edit command:

```
SANbox2 #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created.  If it is not given, the currently active configuration is edited.

Admin mode is required for this command.

  Usage: config edit [CONFIG_NAME]
```

History Command

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority None

Syntax **history**

Notes Use the History command to provide context for the ! command:

- Enter ![command_string] to re-execute the most recent command that matches [command_string].
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples The following is an example of the History command:

```
SANbox2 #> history
   1 show switch
   2 date
   3 help set
   4 history

SANbox2 #> !3
help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:

  Usage: set   { alarm     | beacon    | config    | log       | pagebreak |
                 port      | setup     | switch }
```

Hotreset Command

Resets the switch for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions, saves all configuration information, and clears the event log. After the pending firmware is activated, the configuration is recovered. This process takes less than 80 seconds. To save the event log to a file before resetting, refer to the "Set Log Command" on page B-71.

Authority Admin session

Syntax **hotreset**

Notes

- You can load and activate version 5.0.x firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices under the following conditions:
  - The current firmware version is a 2.0, 3.0, 4.0, 4.1, 4.2, or 5.x version that precedes the upgrade version.
  - No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes.
  - No port in the fabric is in the diagnostic state.
  - No zoning changes are being made in the fabric.
  - No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.
- Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, SANsurfer Switch Manager sessions reconnect automatically. However, Telnet sessions must be restarted manually.
- This command clears the event log and all counters.

Image Command

Manages and installs switch firmware.

Authority Admin session

Syntax

image
cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
install
list
unpack [file]

Keywords

cleanup
Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]
Retrieves image file given by [file_source] and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the FTP server with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the FTP server, the system will prompt you for it.

install
Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch (without a power-on self test) to activate the firmware. If possible, a non-disruptive activation is performed. The command prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

list
Displays the list of image files that reside on the switch.

unpack [file]
Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes

To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

To install firmware when the management workstation has an FTP server, use the Image Install command or the "Firmware Install Command" on page B-23. To install firmware when the management workstation does not have an FTP server, do the following:

1. Connect to the switch through the Ethernet port or the serial port.
2. Move to the folder or directory on the workstation that contains the new firmware image file.
3. Establish communications with the switch using the File Transfer Protocol (FTP). Enter one of the following on the command line:

   ```
   >ftp xxx.xxx.xxx.xxx
   ```

   or

   ```
   >ftp switchname
   ```

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
4. Enter the following account name and password:

   ```
   user:images
   password: images
   ```
5. Activate binary mode and copy the firmware image file on the switch:

   ```
   ftp>bin
   ftp>put filename
   ```
6. Wait for the transfer to complete, then close the FTP session.

   ```
   xxxxx bytes sent in xx secs.
   ftp>quit
   ```
7. Establish communications with the switch using the CLI. Enter one of the following on the command line:

   ```
   telnet xxx.xxx.xxx.xxx
   ```

   or

   ```
   telnet switchname
   ```

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
8. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).

9. Open an Admin session to acquire the necessary authority.

   ```
   SANbox2 $>admin start
   ```

10. Display the list of firmware image files on the switch to confirm that the file was loaded.

    ```
    SANbox2 (admin) $>image list
    ```

11. Unpack the firmware image file to install the new firmware in flash memory.

    ```
    SANbox2 (admin) $>image unpack filename
    ```

12. Wait for the unpack to complete.

    ```
    image unpack command result: Passed
    ```

13. A message will prompt you to reset the switch to activate the firmware. Resetting the switch is disruptive. Use the Hotreset command to attempt a non-disruptive activation.

    ```
    SANbox2 (admin) $>hotreset
    ```

Examples The following is an example of the Image Install command:

```
SANbox2 (admin) #> image install
 Warning: Installing new firmware requires a switch reset.
 Continuing with this action will terminate all management sessions,
 including any Telnet sessions. When the firmware activation is complete,
 you may log in to the switch again.
 Do you want to continue? [y/n]: y
    Press 'q' and the ENTER key to abort this command.

  User Account    : johndoe
  IP Address      : 10.20.33.130
  Source Filename : 5.0.00.11_x86

  About to install image.  Do you want to continue? [y/n] y

Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Lip Command

Reinitializes the specified loop port.

Authority Admin session

Syntax **lip [port_number]**

Keywords **[port_number]**
The number of the port to be reinitialized. Ports are numbered beginning with 0.

Examples The following is an example of the Lip command:

```
SANbox2 (admin) #> lip 2
```

Passwd Command

Changes a user account's password.

Authority Admin account name and an admin session to change another account's password; You can change you own password without an Admin session.

Syntax **passwd [account_name]**

Keywords **[account_name]**
The user account name. To change the password for an account name other than your own, you must open an admin session with the account name Admin. If you omit [account_name], you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
SANbox2 (admin) #> passwd user2

     Press 'q' and the ENTER key to abort this command.

  account OLD password               : ********
  account NEW password (8-20 chars)  : ********

  please confirm account NEW password: ********
  password has been changed.
```

Ping Command

Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority None

Syntax **ping [ip_address]**

Keywords **[ip_address]**
The IP address of the switch to query. Broadcast IP addresses, such as 255.255.255.255, are not valid.

Examples The following is an example of a successful Ping command:

```
SANbox2 #> ping 10.20.11.57
  Ping command issued. Waiting for response...
SANbox2 #>
  Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
SANbox2 #> ping 10.20.10.100
  Ping command issued. Waiting for response...
  No response from 10.20.10.100. Unreachable.
```

Ps Command

Displays current system process information.

Authority None

Syntax **ps**

Examples The following is an example of the Ps command:

```
SANbox2 #> ps


PID  PPID %CPU     TIME     ELAPSED COMMAND
338   327  0.0 00:00:00  3-01:18:35 cns
339   327  0.0 00:00:01  3-01:18:35 ens
340   327  0.0 00:00:21  3-01:18:35 dlog
341   327  0.1 00:05:35  3-01:18:35 ds
342   327  0.2 00:11:29  3-01:18:35 mgmtApp
343   327  0.0 00:00:04  3-01:18:35 fc2
344   327  0.0 00:02:16  3-01:18:35 nserver
345   327  0.0 00:02:44  3-01:18:35 mserver
346   327  0.8 00:35:12  3-01:18:35 util
347   327  0.0 00:00:29  3-01:18:35 snmpservicepath
348   327  0.0 00:02:46  3-01:18:34 eport
349   327  0.0 00:00:21  3-01:18:34 PortApp
350   327  5.6 04:08:24  3-01:18:34 port_mon
351   327  0.0 00:01:38  3-01:18:34 zoning
352   327  0.0 00:00:01  3-01:18:34 diagApp
404   327  0.0 00:00:04  3-01:18:27 snmpd
405   327  0.0 00:00:02  3-01:18:27 snmpmain
406   405  0.0 00:00:00  3-01:18:26 snmpmain
```

Quit Command

Closes the Telnet session.

Authority None

Syntax **quit, exit, or logout**

Notes You can also enter Control-D to close the Telnet session.

Reset Command

Resets the switch configuration parameters. If you omit the keyword, the default is Reset Switch.

Authority Admin session

Syntax **reset**

config *[config_name]*
factory
port [port_number]
radius
security
services
snmp
switch (default)
system
zoning

Keywords **config *[config_name]***

Resets the configuration given by [config_name] to the factory default values for switch, port, port threshold alarm, and zoning configuration as described in Table B-9 through Table B-12. If [config_name] does not exist on the switch, a configuration with that name will be created. If you omit [config_name], the active configuration is reset. You must activate the configuration for the changes to take effect. for switch, port, and port threshold alarm configuration default values.

factory

Resets switch configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, security configuration, RADIUS configuration, switch services configuration, and zoning to the factory default values as described in Table B-9 through Table B-17. The switch configuration is activated automatically.

Note: Because this keyword changes network parameters, the workstation could lose communication with the switch and release the Admin session.

port [port_number]

Reinitializes the port given by [port_number]. Ports are numbered beginning with 0.

radius

Resets the RADIUS configuration to the default values as described in Table B-14.

security

Clears the security database and deactivates the active security set. The security configuration value, autosave, and fabric binding remain unchanged.

services
Resets the switch services configuration to the default values as described in Table B-15.

snmp
Resets the SNMP configuration settings to the factory default values. Refer to Table B-13 for SNMP configuration default values.

switch
Resets the switch without a power-on self test. This is the default. This reset disrupts traffic and does the following:

- Activates the pending firmware.
- Closes all management sessions.
- Clears the event log. To save the event log before resetting, refer to the "Set Log Command" on page B-71.

To reset the switch with a power-on self test, refer to the "Hardreset Command" on page B-32. To reset the switch without disrupting traffic, refer to the "Hotreset Command" on page B-35.

system
Resets the system configuration settings to the factory default values. as described in Table B-16.

Note: ■ Because this keyword changes network parameters, the workstation could lose communication with the switch.

zoning
Clears the zoning database and deactivates the active zone set. The zoning configuration values (autosave, default visibility) remain unchanged.

Notes The following tables specify the various factory default settings:

Enter the Show Config Switch command to display switch configuration values.

Table B-9. Switch Configuration Defaults

Parameter	Default
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1000
DefaultDomain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	SANbox2
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	Config Default
InteropMode	Standard
LegacyAddressFormat	False

Enter the Show Config Port command to display port configuration values.

Table B-10. Port Configuration Defaults

Parameter	Default
Admin State	Online
Link Speed	Auto
Port Type	GL
Symbolic Name	Port n, where n is the port number
ALFairness	False
DeviceScanEnabled	True
ForceOfflineRSCN	False
ARB_FF	False
InteropCredit	0
ExtCredit	0
FANEnable	True
AutoPerfTuning	True
LCFEnable	False
MFSEnable	True
VIEnable	False
MSEnable	True
NoClose	False
IOStreamGuard	Auto
PDISCPingEnable	True

Enter Show Config Threshold command to display threshold alarm configuration values.

Table B-11. Port Threshold Alarm Configuration Defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 25 1 10
DecodeErrorsMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 200 0 10
ISLMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 2 0 10
LoginMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 5 1 10
LogoutMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 5 1 10
LOSMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 100 5 10

Enter the Show Config Zoning command to display zoning configuration values.

Table B-12. Zoning Configuration Defaults

Parameter	Default
InteropAutoSave	True
DefaultVisibility	All
DiscardInactive	False

Enter the Show Setup SNMP command to display SNMP configuration values.

Table B-13. SNMP Configuration Defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	SANbox2-8c FC Switch
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.1663.1.1.1.1.14
AuthFailureTrap	False
ProxyEnabled	True

Enter the Show Setup Radius command to display RADIUS configuration values.

Table B-14. RADIUS Configuration Defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	1
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds

Table B-14. RADIUS Configuration Defaults (Continued)

Parameter	Default
Retries	0
SignPackets	False

Enter the Show Setup Services command to display switch service configuration values.

Table B-15. Services Configuration Defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	True.
MgmtServerEnabled	False

Enter the Show Setup System command to display system configuration values.

Table B-16. System Configuration Defaults

Parameter	Default
Ethernet Network Discovery	Static
Ethernet Network IP Address	10.0.0.1
Ethernet Network IP Mask	255.0.0.0
Ethernet Gateway Address	10.0.0.254
Admin Timeout	30 minutes
InactivityTimeout	0
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Enter the Show Config Security command to display security configuration values.

Table B-17. Security Configuration Defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	True

Security Command

Opens a Security Edit session in which to manage the security database on a switch. Refer to the "Group Command" on page B-24 and the "Securityset Command" on page B-56.

Authority Admin session. The keywords Active, History, Limits, and List are available without an Admin session.

Syntax

security
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays the active security set, its groups, and group members. This keyword does not require an Admin session.

cancel
Closes a Security Edit session without saving changes. Use the Edit keyword to open a Security Edit session.

clear
Clears all inactive security sets from the volatile edit copy of the security database. This keyword does not affect the non-volatile security database. However, if you enter the Security Clear command followed by the Security Save command, the non-volatile security database will be cleared from the switch.

Note: The preferred method for clearing the security database from the switch is the Reset Security command. Refer to the "Reset Command" on page B-44.

edit
Initiates a Security Edit session in which to make changes to the security database. A Security Edit session enables you to use the Group and Securityset commands to create, add, and delete security sets, groups, and group members. To close a Security Edit session and save changes, enter the Security Save command. To close a Security Edit session without saving changes, enter the Security Cancel command.

history
Displays history information about the security database and the active security set including the account name that made changes and when those changes were made. This keyword does not require an Admin session.

limits
Displays the current totals and the security database limits for the number of security sets, groups, members per group, and total members. This keyword does not require an Admin session.

list
Displays all security sets, groups, and group members in the security database. This keyword does not require an Admin session.

restore
Reverts the changes to the security database that have been made during the current Security Edit session since the last Security Save command was entered.

save
Saves the changes that have been made to the security database during a Security Edit session. Changes you make to any security set will not take effect until you activate that security set. Refer to the "Securityset Command" on page B-56 for information about activating a security set.

Examples

The following is an example of the Security Active command:

```
SANbox2 #> security active
  Active Security Information

  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

The following is an example of the Security History command:

```
SB211.192 #> security history
  Active Database Information
  ---------------------------
  SecuritySetLastActivated/DeactivatedBy  Remote
  SecuritySetLastActivated/DeactivatedOn  day month date time year
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@IB-session11
  ConfigurationLastEditedOn           day month date time year
  Database Checksum                   00007558
```

The following is an example of the Security Limits command:

```
SANbox2 #> security limits
  Security Attribute   Maximum   Current   [Name]
  ------------------   -------   -------   ------
  MaxSecuritySets      4         1
  MaxGroups            16        2
  MaxTotalMembers      1000      19
  MaxMembersPerGroup   1000
                                 4         group1
                                 15        group2
```

The following is an example of the Security List command:

```
SANbox2 (admin-security) #> security list
SB211.192 #> security list
  Active Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
              group1 (ISL)
                     10:00:00:00:00:10:21:16
                        Authentication     Chap
                        Primary Hash       MD5
                        Primary Secret     ********
                        Secondary Hash     SHA-1
                        Secondary Secret   ********
                        Binding            0
                     10:00:00:00:00:10:21:17
                        Authentication     Chap
                        Primary Hash       MD5
                        Primary Secret     ********
                        Secondary Hash     SHA-1
                        Secondary Secret   ********
                        Binding            0
```

Securityset Command

Manages security sets in the security database.

Authority Admin session and a Security Edit session. Refer to the "Security Command" on page B-52 for information about starting a Security Edit session. The Active, Groups, and List keywords are available without an Admin session. You must close the Security Edit session before using the Activate and Deactivate keywords.

Syntax

securityset
activate [security_set]
active
add [security_set] [group_list]
copy [security_set_source] [security_set_destination]
create [security_set]
deactivate
delete [security_set]
groups [security_set]
list
remove [security_set] [group]
rename [security_set_old] [security_set_new]

Keywords

activate [security_set]
Activates the security set given by [security_set]. This keyword deactivates the active security set. Close the Security Edit session using the Security Save or Security Cancel command before using this keyword.

active
Displays the name of the active security set. This keyword is available to without an Admin session.

add [security_set] [group_list]
Adds one or more groups given by [group_list] to the security set given by [security_set]. Use a <space> to delimit multiple group names in [group_list]. A security set can have a maximum of three groups with no more than one group of each group type.

copy [security_set_source] [security_set_destination]
Creates a new security set named [security_set_destination] and copies into it the membership from the security set given by [security_set_source].

create [security_set]
Creates the security set with the name given by [security_set]. A security set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 4 security sets.

deactivate
Deactivates the active security set. Close the Security Edit session before using this keyword.

delete [security_set]
Deletes the security set given by [security_set]. If the specified security set is active, the command is suspended until the security set is deactivated.

groups [security_set]
Displays all groups that are members of the security set given by [security_set]. This keyword is available without an Admin session.

list
Displays a list of all security sets. This keyword is available without an Admin session.

remove [security_set] [group]
Removes a group given by [group] from the security set given by [security_set]. If [security_set] is the active security set, the group will not be removed until the security set has been deactivated.

rename [security_set_old] [security_set_new]
Renames the security set given by [security_set_old] to the name given by [security_set_new].

Notes

Refer to the "Group Command" on page B-24 for information about creating and managing groups.

Examples

The following is an example of the Securityset Active command

```
SANbox2 #> securityset active
  Active SecuritySet Information
  ------------------------------
  ActiveSecuritySet alpha
  LastActivatedBy  Remote
  LastActivatedOn  day month date time year
```

The following is an example of the Securityset Groups command

```
SANbox2 #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  --------------------------------------
  group1 (ISL)
  group2 (Port)
```

The following is an example of the Securityset List command

```
SANbox2 #> securityset list
Current list of SecuritySets
----------------------------
  alpha
  beta
```

Set Command

Sets a variety of switch parameters.

Authority Admin session for all keywords except Alarm, Beacon, and Pagebreak which are available without an Admin session.

Syntax

set
alarm [option]
beacon [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]
timezone

Keywords

alarm [option]
Controls the display of alarms in the session output stream or clears the alarm log. [option] can be one of the following:

clear
Clears the alarm log history. This value requires an Admin session.

on
Enables the display of alarms in the session output stream.

off
Disables the display of alarms in the session output stream.

beacon [state]
Enables or disables the flashing of the Logged-In LEDs according to [state]. This keyword does not require an admin session. [state] can be one of the following:

on
Enables the flashing beacon.

off
Disables the flashing beacon.

config [option]
Sets switch, port, port threshold alarm, security, and zoning configuration parameters. Refer to the "Set Config Command" on page B-60.

log [option]
Specifies the type of entries to be entered in the event log. Refer to the "Set Log Command" on page B-71.

pagebreak [state]
Specifies how much information is displayed on the screen at a time according to the value given by [state]. This keyword does not require an admin session. [state] can be one of the following:

on
Limits the display of information to 20 lines at a time. The page break functions affects the following commands: Alias (List, Members), Show (Alarm, Log), Zone (List, Members), Zoneset (List, Zones), Zoning (Active, List).

off
Allows continuous display of information without a break.

port [option]
Sets port state and speed for the specified port. The previous Set Config Port settings are restored after a switch reset or a reactivation of a switch configuration. Refer to the "Set Port Command" on page B-75.

setup [option]
Changes SNMP and system configuration settings. Refer to the "Set Setup Command" on page B-77.

switch [state]
Changes the administrative state for all ports on the switch to the state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [state] can be one of the following:

online
Places all ports online

offline
Places all ports offline.

diagnostics
Prepares all ports for testing.

timezone
Specifies the time zone for the switch and the workstation. The default is Universal Time (UTC) also known as Greenwich Mean Time (GMT). This keyword prompts you to choose a region, then a subregion to specify the time zone.

Examples

The following examples enables and disables the beacon:

```
SANbox2 #> set beacon on

  Command succeeded.

SANbox2 $> set beacon off

  Command succeeded.
```

Set Config Command

Sets switch, port, port threshold alarm, security, and zoning configuration parameters. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command. Refer to the "Config Command" on page B-16.

Authority Admin session and a Config Edit session

Syntax

set config
port *[port_number]*
ports *[port_number]*
security
switch
threshold
zoning

Keywords

port *[port_number]*
Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter "q" to end the configuration for one port, or "qq" to end the configuration for all ports. Table B-18 describes the port parameters.

ports *[port_number]*
Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter "q" to end the configuration. Table B-18 describes the port parameters.

Table B-18. Set Config Port Parameters

Parameter	Description
AdminState	Port administrative state: ■ Online – Activates and prepares the port to send data. This is the default. ■ Offline – Prevents the port from receiving signal and accepting a device login. ■ Diagnostics – Prepares the port for testing and prevents the port from accepting a device login. ■ Down – Disables the port by removing power from the port lasers.
LinkSpeed	Transmission speed: 1-Gbps, 2-Gbps, or Auto. The default is Auto.
PortType	Port type: GL, G, F, FL, Donor. The default is GL.

Table B-18. Set Config Port Parameters (Continued)

Parameter	Description
SymbolicPortName	Descriptive name for the port. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Port n where n is the port number.
ALFairness	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop. The default is False.
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and a device is interrupted. If enabled, the RSCN message is delayed for 200 ms for locally attached devices and 400 ms for devices connected through other switches. The default is False. This parameter is ignored if IOStreamGuard is enabled.
ARB_FF	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default (12) is unchanged. Changing interoperability credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.
ExtCredit	Extended credits. The number of port buffer credits that this port can acquire from donor ports. The default is 0.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.
AutoPerfTuning	Automatic performance tuning for FL_Ports only. The default is True. ■ If AutoPerfTuning is enabled (True) and the port is an FL_Port, MFSEnable is automatically enabled. LCFEnable and VIEnable are overridden to False. ■ If AutoPerfTuning is disabled (False), MFSEnable, LCFEnable, and VIEnable retain their original values.

Table B-18. Set Config Port Parameters (Continued)

Parameter	Description
LCFEnable	Link control frame preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.
MFSEnable	Multi-Frame Sequence bundling. This parameter appears only if AutoPerfTuning is False. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is True. Enabling MFSEnable disables LCFEnable and VIEnable.
VIEnable	Virtual Interface (VI) preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.
NoClose	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.
IOStreamGuard	I/O Stream Guard. Enables or disables the suppression of RSCN messages. IOStreamGuard can have the following values: ■ Enable – Suppresses the reception of RSCN messages from other ports for which IOStreamGuard is enabled. ■ Disable – Allows free transmission and reception of RSCN messages. ■ Auto – Suppresses the reception of RSCN messages when the port is connected to an initiator device with a QLogic HBA. For older QLogic HBAs, such as the QLA2200, the DeviceScanEnabled parameter must also be enabled. The default is Auto.
PDISCPingEnable	Enables (True) or disables (False) the transmission of ping messages from the switch to all devices on a loop port. The default is True.

security
Initiates an editing session in which to change the security settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” or "Q" to end the editing session. Table B-19 describes the Set Config Security parameters.

Table B-19. Security Configuration Parameters

Parameter	Description
AutoSave	Enables (True) or disables (False) the saving of changes to active security set in the switch’s permanent memory. The default is True.
FabricBindingEnabled	Enables (True) or disables (False) the configuration and enforcement of fabric binding on all switches the fabric. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

switch
Initiates an editing session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table B-20 describes the Set Config Switch parameters.

Table B-20. Set Config Switch Parameters

Parameter	Description
AdminState	Switch administrative state: online, offline, or diagnostics. The default is Online.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the switch over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information. The default is True.
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.

Table B-20. Set Config Switch Parameters (Continued)

Parameter	Description
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.
SymbolicName	Descriptive name for the switch. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is SANbox2.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	Switch configuration description. The configuration description can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Config Default.
InteropMode	Propagates just the active zone set throughout the fabric (Standard, FC-SW-2 compliant) or the entire zoning database (Interop-1, non-compliant). The default is Standard.
LegacyAddressFormat	Available only when the InteropMode parameter is Interop-1, this parameter enables (True) or disables (False) the use of legacy address formatting for interoperating with non-FC-SW-2 switches. The default is False.

threshold
Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its triggers, and sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. Refer to the "Config Command" on page B-16 for information about saving and activating a configuration. Table B-21 describes the Set Config Threshold parameters. The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Table B-21. Set Config Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: ■ CRC errors ■ Decode errors ■ ISL connection count ■ Device login errors ■ Device logout errors ■ Loss-of-signal errors
Rising Trigger	The event count above which a rising trigger alarm is logged. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and again exceeds the rising trigger.
Falling Trigger	The event count below which a falling trigger alarm is logged. The switch will not generate another falling trigger alarm for that event until the count exceeds the rising trigger and descends again below the falling trigger.
Sample Window	The period of time in seconds in which to count events.

zoning
Initiates an editing session in which to change switch zoning attributes. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-22. Set Config Zoning Parameters

Parameter	Description
InteropAutoSave	Available only when the InteropMode parameter is Standard, this parameter enables (True) or disables (False) the saving of changes to active zone set in the switch's permanent memory. Refer to "InteropMode" on page B-64. The default is True. Disabling the Autosave parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Autosave parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Autosave parameter should be enabled in a production environment.
DefaultVisibility	Enables (All) or disables (None) communication among the switch's ports/devices and the fabric in the absence of an active zone set. The default is All.
DiscardInactive	Enables (True) or disables (False) the discarding of all inactive zone sets from that zoning database. Inactive zone sets are all zone sets except the active zone set. The default is False.

Examples

The following is an example of the Set Config Port command:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config port 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------

  AdminState    (1=Online, 2=Offline, 3=Diagnostics, 4=Down)       [Online]
  LinkSpeed     (1=1Gb/s, 2=2Gb/s, 3=Auto)                         [Auto  ]
  PortType      (GL / G / F / FL / Donor)                          [GL    ]
```

```
  SymPortName   (string, max=32 chars)                              [Port1 ]
  ALFairness    (True / False)                                      [False ]
  DeviceScanEnable (True / False)                                   [True  ]
  ForceOfflineRSCN (True / False)                                   [False ]
  ARB_FF        (True / False)                                      [False ]
  InteropCredit (decimal value, 0-255)                              [0     ]
  ExtCredit     (dec value, increments of 11, non-loop only)        [0     ]
  FANEnable     (True / False)                                      [True  ]
  AutoPerfTuning (True / False)                                     [False ]
  LCFEnable     (True / False)                                      [False ]
  MFSEnable     (True / False)                                      [False ]
  VIEnable      (True / False)                                      [False ]
  MSEnable      (True / False)                                      [True  ]
  NoClose       (True / False)                                      [False ]
  IOStreamGuard (Enable / Disable / Auto)                           [Disable]
  PDISCPingEnable  (True / False)                                   [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
SANbox2 (admin-config) #>
```

The following is an example of the Set Config Security command:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config security
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  FabricBindingEnabled  (True / False)     [False]
  AutoSave              (True / False)     [True ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Switch command:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AdminState          (1=Online, 2=Offline, 3=Diagnostics)   [Online        ]
  BroadcastEnabled    (True / False)                         [True          ]
  InbandEnabled       (True / False)                         [True          ]
  FDMIEnabled        (True / False)                          [True         ]
  FDMIEntries        (decimal value, 0-1000)                 [1000         ]
  DefaultDomainID     (decimal value, 1-239)                 [2             ]
  DomainIDLock        (True / False)                         [False         ]
  SymbolicName        (string, max=32 chars)                 [SANbox        ]
  R_A_TOV             (decimal value, 100-100000 msec)       [10000         ]
  E_D_TOV             (decimal value, 10-20000 msec)         [2000          ]
  PrincipalPriority   (decimal value, 1-255)                 [254           ]
  ConfigDescription   (string, max=64 chars)                 [Default Config]
  InteropMode         (0=Standard, 1=Interop_1)              [Standard      ]
```

The following is an example of the Set Config Threshold command:

```
SANbox2 #> admin start
SANbox2  (admin) #> config edit
SANbox2 (admin-config) #> set config threshold
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.
ThresholdMonitoringEnabled     (True / False)              [False     ]

CRCErrorsMonitoringEnabled     (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

DecodeErrorsMonitoringEnabled  (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [200       ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

ISLMonitoringEnabled           (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [2         ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

LoginMonitoringEnabled         (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

LogoutMonitoringEnabled        (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

LOSMonitoringEnabled           (True / False)               [True     ]
  RisingTrigger                (decimal value, 1-1000)      [100     ]
  FallingTrigger               (decimal value, 0-1000)      [5       ]
  SampleWindow                 (decimal value, 1-1000 sec)  [10      ]
Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Zoning command.

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config zoning

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

  InteropAutoSave      (True / False)  [True]
  DefaultVisibility    (All / None)    [All ]
  DiscardInactive      (True / False)  [False]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Log Command

Specifies the events to record in the event log and display on the screen. You determine what events to record in the switch event log using the Component, Level, and Port keywords. You determine what events are automatically displayed on the screen using the Display keyword. Alarms are always displayed on the screen.

Authority Admin session

Syntax

set log
archive
clear
component [filter_list]
display [filter]
level [filter]
port [port_list]
restore
save
start (default)
stop

Keywords

archive
Collects all log entries and stores the result in new file named *logfile* that is maintained in switch memory where it can be downloaded using FTP. To download *logfile*, open an FTP session, log in with account name/password of “images” for both, and type “get logfile”.

clear
Clears all log entries.

component [filter_list]
Specifies one or more components given by [filter_list] to monitor for events. A component is a firmware module that is responsible for a particular portion of switch operation. Use a <space> to delimit values in the list. [filter_list] can be one or more of the following:

All
Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events.

SNMP
Monitors all SNMP events.

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

display [filter]
Specifies the log events to automatically display on the screen according to the event severity levels given by [filter]. [filter] can be one of the following values:

Critical
Critical severity level events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn
Warning severity level events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info
Informative severity level events. The informative level describes routine events associated with a normal fabric.

None
Specifies no severity levels for display on the screen.

level [filter]
Specifies the severity level given by [filter] to use in monitoring and logging events for the specified components or ports. [filter] can be one of the following values:

Critical
Monitors critical events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn
Monitors warning and critical events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info
Monitors informative, warning, and critical events. The informative level describes routine events associated with a normal fabric. This is the default severity level.

None
Monitors none of the severity levels.

port [port_list]
Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]
Specifies port or ports to monitor. Use a <space> to delimit values in the list. Ports are numbered beginning with 0.

All
Specifies all ports.

None
Disables monitoring on all ports.

restore
Restores and saves the port, component, and level settings to the default values.

save
Saves the log settings for the component, severity level, port, and display level. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start
Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop
Stops logging of events.

Notes In addition to critical, warn, and informative severity levels, the highest event severity level is alarm. The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen.

Set Port Command

Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters.

Authority Admin session except for the Clear keyword.

Syntax

set port [port_number]
bypass [alpa]
clear
enable
speed [transmission_speed]
state [state]

Keywords

[port_number]
Specifies the port. Ports are numbered beginning with 0.

bypass [alpa]
Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear
Clears the counters on the port. This keyword does not require an admin session.

enable
Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]
Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s
One gigabit per second.

2Gb/s
Two gigabits per second.

Auto
The port speed is automatically detected.

state [state]
Specifies one of the following administrative states for the specified port:

Online
Places the port online. This activates and prepares the port to send data.

Offline
Places the port offline. This prevents the port from receiving signal and accepting a device login.

Diagnostics
Prepares the port for testing. This prepares the port for testing and prevents the port from accepting a device login.

Down
Disables the port by removing power from the port lasers.

Set Setup Command

Manages configuration settings for Remote Authentication Dial-In User Service (RADIUS) servers, switch services, SNMP, and system configurations.

Authority Admin session

Syntax **set setup**
radius
services
snmp
system

Keywords **radius**
Prompts you in a line-by-line fashion to configure RADIUS servers for user account and device authentication. Table B-23 describes the RADIUS server configuration fields.

Table B-23. RADIUS Service Settings

Entry	Description
DeviceAuthOrder	Authenticator priority for devices: ■ Local: Authenticate devices using only the local security database. This is the default. ■ Radius: Authenticate devices using only the security database on the RADIUS server. ■ RadiusLocal: Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
UserAuthOrder	Authenticator priority for user accounts: ■ Local: Authenticate users using only the local security database. This is the default. ■ Radius: Authenticate users using only the security database on the RADIUS server. ■ RadiusLocal: Authenticate users using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
TotalServers	Number of RADIUS servers to configure during this session. Setting TotalServers to 0 disables all RADIUS authentication. The default is 0.
ServerIPAddress	IP address of the RADIUS server. The default is 10.0.0.1.
ServerUDPPort	User Datagram Protocol (UDP) port number on the RADIUS server. The default is 1812.

Table B-23. RADIUS Service Settings (Continued)

Entry	Description
DeviceAuthServer	Enable (True) or disable (False) this server for device authentication. The default is False.
UserAuthServer	Enable (True) or disable (False) this server for user account authentication. A user authentication RADIUS server requires a secure management connection (SSL). The default is True.
AccountingServer	Enable (True) or disable (False) this server for auditing of activity during a user session. When enabled, user activity is audited whether UserAuthServer is enabled or not.The default is False. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).
Timeout	Number of seconds to wait to receive a response from the RADIUS server before timing out. The default is 2.
Retries	Number of retries after the first attempt to establish communication with the RADIUS server fails. The default is 0.
SignPackets	Enable (True) or disable (False) the use of sign packets to protect the RADIUS server packet integrity. The default is False.
Secret	32-byte hex string or 16-byte ASCII string used as a password for authentication purposes between the switch and the RADIUS server.

services
Prompts you in a line-by-line fashion to enable or disable switch services. Table B-24 describes the switch service parameters. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Note: Use caution when disabling TelnetEnabled and GUIMgmtEnabled; it is possible to disable all Ethernet access to the switch.

Table B-24. Switch Services Settings

Entry	Description
TelnetEnabled	Enables (True) or disables (False) the ability to manage the switch over a Telnet connection. Disabling this service is not recommended. The default is True.
SSHEnabled	Enables (True) or disables (False) Secure Shell (SSH) connections to the switch. SSH secures the remote connection to the switch. To establish a secure remote connection, your workstation must use an SSH client. The default is False.
GUIMgmtEnabled	Enables (True) or disables (False) out-of-band management of the switch with SANsurfer Switch Manager, the SANsurfer Switch Manager Application Application Programming Interface, SNMP, and CIM. If this service is disabled, the switch can only be managed inband or through the serial port. The default is True.
SSLMgmtEnabled	Enables (True) or disables (False) secure SSL connections for management applications including SANsurfer Switch Manager, the SANsurfer Switch Manager web applet, SANsurfer Switch Manager Application Programming Interface, and the CIM server. The default is False. ■ To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. ■ This service must be enabled to authenticate users through a RADIUS server. ■ Enabling SSL automatically creates a security certificate on the switch. ■ To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.

Table B-24. Switch Services Settings (Continued)

Entry	Description
EmbeddedGUIEnabled	Enables (True) or disables (False) the SANsurfer Switch Manager web applet. The web applet enables you to point at a switch with an internet browser and run SANsurfer Switch Manager through the browser. This parameter is the master control for the Set Setup System command parameter, EmbeddedGUIEnabled. The default is True.
SNMPEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). This parameter is the master control for the Set Setup SNMP command parameter, SNMPEnabled. The default is True.
NTPEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) which allows the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is False. This parameter is the master control for the Set Setup System command parameter, NTPClientEnabled. The default is False.
CIMEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use the Common Information Model (CIM). The default is True.
FTPEnabled	Enables (True) or disables (False) the File Transfer Protocol (FTP) for transferring files rapidly between the workstation and the switch. The default is True.
MgmtServerEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use GS-3 Management Server (MS). This parameter is the master control for the Set Config Port command parameter, MSEnable. The default is False.

snmp
Prompts you in a line-by-line fashion to change SNMP configuration settings. Table B-25 describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-25. SNMP Configuration Settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the switch. The default is True.
Contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Location	Specifies the name of the switch location. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is 162.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning.
Trap [1-5] Version	Specifies the SNMP version (1 or 2) to use in formatting traps. The default is 2.
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The write community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “private”.

Table B-25. SNMP Configuration Settings (Continued)

Entry	Description
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

system
Prompts you in a line-by-line fashion to change system configuration settings. Table B-26 describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Note: Changing the IP address will terminate all Ethernet management sessions.

Table B-26. System Configuration Settings

Entry	Description
Eth0NetworkDiscovery	Ethernet boot method: 1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP. The default is 1 - Static.
Eth0NetworkAddress	Ethernet Internet Protocol (IP) address. The default is 10.0.0.1.
Eth0NetworkMask	Ethernet subnet mask address.
Eth0GatewayAddress	Ethernet IP address gateway.
AdminTimeout	Amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
InactivityTimeout	Amount of time in minutes the switch waits before terminating an idle Telnet command line interface session. Zero (0) disables the time out threshold. The default is 0, the maximum is 1440.

Table B-26. System Configuration Settings (Continued)

Entry	Description
LocalLogEnabled	Enables (True) or disables (False) the saving of log information on the switch. The default is True.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address of the host that will receive the switch event log information if remote logging is enabled. The default is 10.0.0.254.
NTPClientEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) client on the switch. This client enables the switch to synchronize its time with an NTP server. This feature supports NTP version 4 and is compatible with version 3. An Ethernet connection to the server is required and you must first set an initial time and date on the switch. The synchronized time becomes effective immediately. The default is False.
NTPServerAddress	The IP address of the NTP server from which the NTP client acquires the time and date. The default is 10.0.0.254.
EmbeddedGUIEnabled	Enables (True) or disables (False) the SANsurfer Switch Manager Web applet. Changing this parameter to False while the applet is running will terminate the applet. The default is True.

Examples

The following is an example of the Set Setup RADIUS command:

```
SANbox2 (admin) #> set setup radius
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the attributes
  for the server being processed, press 'q' or 'Q' and the ENTER key to do so.
  If you wish to terminate the configuration process completely, press 'qq' or
  'QQ' and the ENTER key to so do.

  DeviceAuthOrder   (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  UserAuthOrder     (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  TotalServers      (decimal value, 0-5)               [1    ]

  Server: 1
  ServerIPAddress   (dot-notated IP Address)         [10.20.11.8]
  ServerUDPPort     (decimal value)                  [1812      ]
```

```
DeviceAuthServer  (True / False)                  [True      ]
UserAuthServer    (True / False)                  [True      ]
AccountingServer  (True / False)                  [False     ]
Timeout           (decimal value, 10-30 secs)     [10        ]
Retries           (decimal value, 1-3, 0=None)    [0         ]
SignPackets       (True / False)                  [False     ]
Secret            (32 hex or 16 ASCII char value) [********  ]
Do you want to save and activate this radius setup? (y/n): [n]
```

The following is an example of the Set Setup Services command:

```
SANbox2 (admin) #> set setup services

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

*Warning: If services are disabled, the connection to the switch may be lost.


TelnetEnabled       (True / False)       [True ]
SSHEnabled          (True / False)       [False]
GUIMgmtEnabled      (True / False)       [True ]
SSLMgmtEnabled      (True / False)       [False]
EmbeddedGUIEnabled  (True / False)       [True ]
SNMPEnabled         (True / False)       [True ]
NTPEnabled          (True / False)       [False]
CIMEnabled          (True / False)       [True ]
FTPEnabled          (True / False)       [True ]
MgmtServerEnabled   (True / False)       [True ]


Do you want to save and activate this services setup? (y/n): [n]
```

The following is an example of the Set Setup SNMP command:

```
SANbox2 #> admin start
SANbox2 (admin) #> set setup snmp
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Trap Severity Options
  ---------------------
  unknown, emergency, alert, critical, error, warning, notify, info, debug, mark
  SNMPEnabled         (True / False)               [True             ]
  Contact             (string, max=64 chars)      [<sysContact undefined]
  Location            (string, max=64 chars)      [sysLocation undefined]
  Trap1Address        (dot-notated IP Address)    [10.20.71.15      ]
  Trap1Port           (decimal value)             [162              ]
  Trap1Severity       (see allowed options above) [warning          ]
  Trap1Version        (1 / 2)                     [2                ]
  Trap1Enabled        (True / False)              [False            ]
  Trap2Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap2Port           (decimal value)             [162              ]
  Trap2Severity       (see allowed options above) [warning          ]
  Trap2Version        (1 / 2)                     [2                ]
  Trap2Enabled        (True / False)              [False            ]
  Trap3Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap3Port           (decimal value)             [162              ]
  Trap3Severity       (see allowed options above) [warning          ]
  Trap3Version        (1 / 2)                     [2                ]
  Trap3Enabled        (True / False)              [False            ]
  Trap4Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap4Port           (decimal value)             [162              ]
  Trap4Severity       (see allowed options above) [warning          ]
  Trap4Version        (1 / 2)                     [2                ]
  Trap4Enabled        (True / False)              [False            ]
  Trap5Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap5Port           (decimal value)             [162              ]
  Trap5Severity       (see allowed options above) [warning          ]
  Trap5Version        (1 / 2)                     [2                ]
  Trap5Enabled        (True / False)              [False            ]
  ReadCommunity       (string, max=32 chars)      [public           ]
  WriteCommunity      (string, max=32 chars)      [private          ]
  TrapCommunity       (string, max=32 chars)      [public           ]
  AuthFailureTrap     (True / False)              [False            ]
  ProxyEnabled        (True / False)              [True             ]
```

The following is an example of the Set Setup System command:

```
SANbox2 (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

Eth0NetworkDiscovery    (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
Eth0NetworkAddress      (dot-notated IP Address)             [10.0.0.1     ]
Eth0NetworkMask         (dot-notated IP Address)             [255.255.255.0]
Eth0GatewayAddress      (dot-notated IP Address)             [10.0.0.254   ]
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
InactivityTimeout       (dec value 0-1440 minutes, 0=never)  [0            ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
NTPClientEnabled        (True / False)                       [False        ]
NTPServerAddress        (dot-notated IP Address)             [10.0.0.254   ]
EmbeddedGUIEnabled      (True / False)                       [True         ]
```

Show Command

Displays fabric, switch, and port operational information.

Authority None

Syntax **show**

about
alarm *[option]*
audit
broadcast
chassis
cimlistener *[listener_name]*
cimsubscription *[subscription_name]*
config [option]
domains
donor
fabric
fdmi *[port_wwn]*
interface
log *[option]*
lsdb
mem [count]
ns *[option]*
pagebreak
perf *[option]*
port *[port_number]*
post log
setup [option]
steering *[domain_id]*
support
switch
timezone
topology
users
version

Keywords **about**

Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the Version keyword.

alarm *[option]*
Displays the alarm log and session display setting. If you omit [option], the command displays the last 200 alarm entries. The alarm log is cleared when the switch is reset or power cycled. [option] has the following value:

setting
Displays the status of the parameter that controls the display of alarms in the session output stream. This parameter is set using the Set Alarm command.

audit
Displays the most recent 200 records in the administrative audit log. The audit log contains configuration and administrative changes that have been made to the switch including the originating management session and IP address.

broadcast
Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis
Displays chassis component status and temperature.

cimlistener *[listener_name]*
Displays CIM indicator services listener information for the listener given by [listener_name]. If you omit [listener_name], the command displays all listeners.

cimsubscription *[subscription_name]*
Displays CIM subscription information for the subscription given by [subscription_name]. If you omit [subscription_name], the command displays all subscriptions.

config [option]
Displays switch, port, and zoning configuration attributes. Refer to the "Show Config Command" on page B-102.

domains
Displays list of each domain and its worldwide name in the fabric.

donor
Displays list of current donor configuration for all ports.

fabric
Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address.

fdmi *[port_wwn]*
Displays detailed information about the device host bus adapter given by [port_wwn]. If you omit [port_wwn], the command displays a summary of host bus adapter information for all attached devices in the fabric. Illegal characters in the display appear as question marks (?).

interface
Displays the status of the active network interfaces.

log *[option]*
Displays log entries. Refer to the “Show Log Command” on page B-105. The log is cleared when the switch is reset or power cycled.

lsdb
Displays Link State database information

mem [count]
Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

> ***Note:*** This keyword will display memory activity updates until [count] is reached – it cannot be interrupted. Therefore, avoid using large values for [count].

ns *[option]*
Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all
Displays name server information for all switches and ports.

[domain_id]
Displays name server information for the switch given by [domain_id]. [domain_id] is a switch domain ID.

[port_id]
Displays name server information for the port given by [port_id]. [port_id] is a port Fibre Channel address.

pagebreak
Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

perf *[option]*
Displays performance information for all ports. Refer to the “Show Perf Command” on page B-108.

port *[port_number]*
Displays operational information for the port given by [port_number]. Ports are numbered beginning with 0. If [port number] is omitted, information is displayed for all ports. Table B-27 describes the port parameters.

Table B-27. Show Port Parameters

Entry	Description
AInit	Incremented each time the port begins AL initialization.
AInitError	Number of times the port entered initialization and the initialization failed.
Bad Frames	Number of frames that have framing errors.
ClassXFramesIn	Number of class *x* frames received by this port.
ClassXFramesOut	Number of class *x* frames sent by this port.
ClassXWordsIn	Number of class *x* words received by this port.
ClassXWordsOut	Number of class *x* words sent by this port.
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF.
DecodeError	Number of decode errors detected
EpConnects	Number of times an E_Port connected through ISL negotiation.
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowerrors	Received a frame when there were no available credits.
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.
InvalidDestAddr	Invalid destination address detected.
LIP_AL_PD_ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIP_F7_AL_PS	This LIP is used to reinitialize the loop. An L_Port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.

Table B-27. Show Port Parameters (Continued)

Entry	Description
LIP_F8_AL_PS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS.
LIP_F7_F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIP_F8_F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
Login	Number of device logins
Logout	Number of device logouts
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
PrimSeqErrors	Primitive sequence errors detected.
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
TotalErrors	Total number of errors detected.
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port.
TotalLinkResets	Total number of link reset primitives.
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.

Table B-27. Show Port Parameters (Continued)

Entry	Description
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Total number of Offline Sequences issued by this port.

post log
Displays the Power On Self Test (POST) log which contains results from the most recently failed POST.

setup [option]
Displays setup attributes for the system, SNMP, and the switch manufacturer. Refer to the "Show Setup Command" on page B-110.

steering *[domain_id]*
Displays the routes that data takes to the switch given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

support
Executes a series of commands that display a complete description of the switch, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This keyword is intended for use at the request of your authorized maintenance provider. The commands that are executed include the following:

- Alias List
- Config List
- Date
- Group List
- History
- Ps
- Security (List, Limits, History)
- Securityset (Active, List)
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Security, Config Switch, Config Threshold, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Archive, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts

- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

switch
Displays switch operational information.Table B-28 describes the switch operational parameters.

Table B-28. Switch Operational Parameters

Parameter	Description
SymbolicName	Descriptive name for the switch
SwitchWWN	Switch world wide name
SwitchType	Switch model
BootVersion	PROM boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch domain ID
FirstPortAddress	FC address of switch port 0
FlashSize - MBytes	Size of the flash memory in megabytes
LogLevel	Event severity level used to record events in the event log
MaxPorts	Number of ports available on the switch
NumberOfResets	Number of times the switch has been reset over its service life
ReasonForLastReset	Action that caused the last reset
ActiveImageVersion - build date	Active firmware image version and build date.
PendingImageVersion - build date	Firmware image version and build date that is pending. This image will become active at the next reset or power cycle.
ActiveConfiguration	Name of the switch configuration that is in use.
AdminState	Switch administrative state
AdminModeActive	Admin session status

Table B-28. Switch Operational Parameters (Continued)

Parameter	Description
BeaconOnStatus	Beacon status as set by the Set Beacon command.
OperationalState	Switch operational state
PrincipalSwitchRole	Principal switch status. True indicates that this switch is the principal switch.
BoardTemp (1) - Degrees Celsius	Internal switch temperature at circuit board sensor 1
BoardTemp (2) - Degrees Celsius	Internal switch temperature at circuit board sensor 2
SwitchDiagnosticsStatus	Results of the power-on self test
SwitchTemperatureStatus	Switch temperature status: normal, warning, failure

timezone
Displays the current time zone setting.

topology
Displays all connected devices.

users
Displays a list of logged-in users. This is equivalent to the User List command.

version
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the About keyword.

Examples

The following is an example of the Show Chassis command:

```
SANbox2 #> show chassis
  Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   34
  BoardTemp (2) - Degrees Celsius   31
  FanStatus (1)                     Good
  PowerSupplyStatus (1)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

The following is an example of the Show Domains command:

```
SANbox2 #> show domains
  Principal switch is (remote): 10:00:00:60:69:50:0b:6c
  Upstream Principal ISL is   : 1
  Domain ID List:
        Domain 97  (0x61)  WWN = 10:00:00:c0:dd:00:71:ed
        Domain 98  (0x62)  WWN = 10:00:00:60:df:22:2e:0c
        Domain 99  (0x63)  WWN = 10:00:00:c0:dd:00:72:45
        Domain 100 (0x64)  WWN = 10:00:00:c0:dd:00:ba:68
        Domain 101 (0x65)  WWN = 10:00:00:60:df:22:2e:06
        Domain 102 (0x66)  WWN = 10:00:00:c0:dd:00:90:ef
        Domain 103 (0x67)  WWN = 10:00:00:60:69:50:0b:6c
        Domain 104 (0x68)  WWN = 10:00:00:c0:dd:00:b8:b7
```

The following is an example of the Show Fabric command:

```
SANbox2 #> show fabric

 Domain     WWN                     Enet IP Addr    FC IP Addr      SymbolicName
 ------     ---                     ------------    ----------      ------------
 16 (0x10)  10:00:00:c0:dd:00:77:81 10.20.68.11     0.0.0.0         gui sb1 .11
 17 (0x11)  10:00:00:c0:dd:00:6a:2d 10.20.68.12     0.0.0.0         sw12
 18 (0x12)  10:00:00:c0:dd:00:c3:04 10.20.68.160    0.0.0.0         sw .160
 19 (0x13)  10:00:00:c0:dd:00:bc:56 10.20.68.108    0.0.0.0         Sb2 .108
```

The following is an example of the Show FDMI command:

```
SANbox2 #> show fdmi

HBA ID                  PortID  Manufacturer           Model    Ports
--------                ------  ---------------       -------   -----
21:01:00:e0:8b:27:aa:bc 610000  QLogic Corporation    QLA2342   2
21:00:00:00:ca:25:9b:96 180100  QLogic Corporation    QL2330    2
```

The following is an example of the Show FDMI WWN command:

```
SANbox2 #> show fdmi 21:00:00:e0:8b:09:3b:17
  FDMI Information
  ----------------
  Manufacturer            QLogic Corporation
  SerialNumber            [04202
  Model                   QLA2342
  ModelDescription        QLogic QLA2342 PCI Fibre Channel Adapter
  PortID                  610000
  NodeWWN                 20:00:00:e0:8b:07:aa:bc
  HardwareVersion         FC5010409-10
  DriverVersion           8.2.3.10 Beta 2 (W2K VI)
  OptionRomVersion        1.21
  FirmwareVersion         03.02.13.
  OperatingSystem         SunOS 5.8
  MaximumCTPayload        2040
  NumberOfPorts           1

  Port  21:01:00:e0:8b:27:aa:bc

  SupportedFC4Types       FCP
  SupportedSpeed          2Gb/s
  CurrentSpeed            2Gb/s
  MaximumFrameSize        2048
  OSDeviceName
  HostName
```

The following is an example of the Show NS (local domain) command:

```
SANbox2 #> show ns
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   19 (0x13) 1301e1 NL   3   21:00:00:20:37:73:13:69 20:00:00:20:37:73:13:69
  2   19 (0x13) 1301e2 NL   3   21:00:00:20:37:73:12:9b 20:00:00:20:37:73:12:9b
  3   19 (0x13) 1301e4 NL   3   21:00:00:20:37:73:05:26 20:00:00:20:37:73:05:26
  4   19 (0x13) 130d00 N    3   21:01:00:e0:8b:27:a7:bc 20:01:00:e0:8b:27:a7:bc
```

The following is an example of the Show NS [domain_ID] command:

```
SANbox2 #> show ns 18
    Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   18 (0x12) 120700 N    3   21:00:00:e0:8b:07:a7:bc 20:00:00:e0:8b:07:a7:bc
```

The following is an example of the Show NS [port_ID] command:

```
SANbox2 #> show ns 1301e1
  Port ID: 1301e1
  --------
  PortType          NL
  PortWWN           21:00:00:20:37:73:13:69
  SymbolicPortName
  NodeWWN           20:00:00:20:37:73:13:69
  SymbolicNodeName
  NodeIPAddress     0.0.0.0
  ClassOfService    3
  PortIPAddress     0.0.0.0
  FabricPortName    20:01:00:c0:dd:00:bc:56
  FC4Type           FCP
  FC4Desc           (NULL)
```

The following is an example of the Show Interface command:

```
SANbox2 #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:00:BD:ED
          inet addr:10.20.68.107  Bcast:10.20.68.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4712 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:415313 (405.5 Kb)  TX bytes:716751 (699.9 Kb)
          Interrupt:11 Base address:0xfcc0
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20116 (19.6 Kb)  TX bytes:20116 (19.6 Kb)
```

The following is an example of the Show Port command:

```
SANbox2 #> show port 1
  Port Number: 1
  ------------
  AdminState       Online             OperationalState Online
  AsicNumber       0                  PerfTuningMode   Normal
  AsicPort         1                  PortID           0e0800
  ConfigType       GL                 PortWWN          20:08:00:c0:dd:03:d5:94
  DiagStatus       Passed             RunningType      E
  EpConnState      Connected          MediaPartNumber  PL-XPL-VC-SG3-22
  EpIsoReason      NotApplicable      MediaRevision    1
  IOStreamGuard    Disabled           MediaType        200-M5-SN-I
  LinkSpeed        2Gb/s              MediaVendor      Unknown
  LinkState        Active             MediaVendorID    00000485
  LoginStatus      LoggedIn           SymbolicName     Port8
  MaxCredit        12                 SyncStatus       SyncAcquired
  MediaSpeeds      1Gb/s, 2Gb/s       XmitterEnabled   True

  ALInit          5                    LIP_F8_AL_PS    0
  ALInitError     0                    LIP_F8_F7       0
  BadFrames       0                    LinkFailures    2
  Class2FramesIn  0                    Login           3
  Class2FramesOut 0                    Logout          2
  Class2WordsIn   0                    LoopTimeouts    1
  Class2WordsOut  0                    LossOfSync      2
  Class3FramesIn  999                  PrimSeqErrors   0
  Class3FramesOut 540                  RxLinkResets    1
  Class3Toss      0                    RxOfflineSeq    0
  Class3WordsIn   29516                TotalErrors     628777
  Class3WordsOut  8406                 TotalLinkResets 6
  DecodeErrors    628775               TotalLIPsRecvd  5
  EpConnects      3                    TotalLIPsXmitd  7
  FBusy           0                    TotalOfflineSeq 5
  FlowErrors      0                    TotalRxFrames   999
  FReject         0                    TotalRxWords    29516
  InvalidCRC      0                    TotalTxFrames   540
  InvalidDestAddr 0                    TotalTxWords    8406
  LIP_AL_PD_AL_PS 0                    TxLinkResets    5
  LIP_F7_AL_PS    0                    TxOfflineSeq    5
  LIP_F7_F7       5
```

The following is an example of the Show Switch command:

```
SANbox2 #> show switch
Switch Information
------------------
SymbolicName                     sw .108
SwitchWWN                        100000c0dd00bc56
SwitchType                       SANbox2-8c
BootVersion                      Vx.x.x.x-0 (day month date time year)
CreditPool                       0
DomainID                         19 (0x13)
FirstPortAddress                 130000
FlashSize - MBytes               128
LogLevel                         Critical
MaxPorts                         8
NumberOfResets                   15
ReasonForLastReset               PowerUp
ActiveImageVersion - build date  Vx.x.x.0-2 (day month date time year)
PendingImageVersion - build date Vx.x.x.0-17 (day month date time year)
ActiveConfiguration              default
AdminState                       Online
AdminModeActive                  False
BeaconOnStatus                   False
OperationalState                 Online
PrincipalSwitchRole              False
BoardTemp (1) - Degrees Celsius  32
BoardTemp (2) - Degrees Celsius  36
SwitchDiagnosticsStatus          Passed
SwitchTemperatureStatus          Normal
```

The following is an example of the Show Topology command:

```
SANbox2 #> show topology
Unique ID Key
-------------
A = ALPA,  D = Domain ID,  P = Port ID
Port   Local Local                    Remote  Remote                    Unique
Number Type  PortWWN                  Type    NodeWWN                   ID
------ ----- -------                  ------  -------                   ------
5      F     20:05:00:c0:dd:00:bd:ec   N      20:00:00:00:c9:22:1e:93   010500 P
10     E     20:0a:00:c0:dd:00:bd:ec   E      10:00:00:c0:dd:00:80:21   4(0x4) D
```

The following is an example of the Show Topology command for port 1:

```
SANbox2  #> show topology 1
  Local Link Information
  ----------------------
  PortNumber 1
  PortID     650100
  PortWWN    20:01:00:c0:dd:00:91:11
  PortType   F

Remote Link Information
-----------------------
Device 0
NodeWWN 50:80:02:00:00:06:d5:38
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 1
NodeWWN 20:00:00:20:37:2b:08:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 2
Description (NULL)
IPAddress 0.0.0.0

Device 3
NodeWWN 20:00:00:20:37:2b:05:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0
```

The following is an example of the Show Version command:

```
SANbox2 #> show version
       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription     SANbox2-8c FC Switch
       Eth0NetworkAddress    10.20.11.192 (use 'set setup system' to update)
       MACAddress            00:c0:dd:00:71:ee
       WorldWideName         10:00:00:c0:dd:00:71:ed
       ChassisSerialNumber   FAM033100024
       SymbolicName          SANbox2
       ActiveSWVersion       V5.0.x.x.xx.xx
       ActiveTimestamp       day month date time year
       DiagnosticsStatus     Passed
```

Show Config Command

Displays switch, port, alarm threshold, security, and zoning for the current configuration.

Authority None

Syntax **show config**
port *[port_number]*
security
switch
threshold
zoning

Keywords **port *[port_number]***
Displays configuration parameters for the port number given by [port_number]. Ports are numbered beginning with 0. If [port_number] is omitted, all ports are specified.

security
Displays the security database Autosave parameter value.

switch
Displays configuration parameters for the switch.

threshold
Displays alarm threshold parameters for the switch.

zoning
Displays zoning configuration parameters for the switch.

Examples The following is an example of the Show Config Port command:

```
SANbox2 #> show config port 3
    Port Number: 3
  ------------
  AdminState         Offline
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port3
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  AutoPerfTuning     False
  LCFEnabled         False
  MFSEnabled         True
```

```
  MSEnabled          True
  NoClose            False
  IOStreamGuard      Disabled
  VIEnabled          False
  PDISCPingEnable    True
```

The following is an example of the Show Config Switch command:

```
SANbox2 #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DomainID              19 (0x13)
  DomainIDLock          True
  SymbolicName          sw108
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

The following is an example of the Show Config Threshold command:

```
SANbox2 #> show config threshold
Configuration Name: default
------------
  Threshold Configuration Information
-----------------------------------
ThresholdMonitoringEnabled    False
CRCErrorsMonitoringEnabled    True
RisingTrigger                 25
FallingTrigger                1
SampleWindow                  10
DecodeErrorsMonitoringEnabled True
RisingTrigger                 25
FallingTrigger                0
SampleWindow                  10
ISLMonitoringEnabled          True
RisingTrigger                 2
FallingTrigger                0
SampleWindow                  10
LoginMonitoringEnabled        True
RisingTrigger                 5
FallingTrigger                1
SampleWindow                  10
LogoutMonitoringEnabled       True
RisingTrigger                 5
FallingTrigger                1
SampleWindow                  10
LOSMonitoringEnabled          True
RisingTrigger                 100
FallingTrigger                5
SampleWindow                  10
```

The following is an example of the Show Config Zoning command:

```
SANbox2 #> show config zoning
 Configuration Name: default
  -------------------
  Zoning Configuration Information
  --------------------------------
  InteropAutoSave       True
  DefaultVisibility     All
  DiscardInactive       False
```

Show Log Command

Displays the contents of the log or the parameters used to create and display entries in the log. The log contains a maximum of 1200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority None

Syntax **show log**
[number_of_events]
component
display [filter]
level
options
port
settings

Keywords **[number_of_events]**
Specifies the number of the most recent events to display from the event log. [number_of_events] must be a positive integer.

component
Displays the components currently being monitored for events. The components are as follows:

All
Monitors all components.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events

SNMP
SNMP events.

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

display [filter]
Displays log events on the screen according to the component or severity level filter given by [filter]. [filter] can be one of the following:

Info
Displays all informative events.

Warning
Displays all warning events.

Critical
Displays all critical events.

Eport
Displays all events related to E_Ports.

Mgmtserver
Displays all events related to the management server.

Nameserver
Displays all events related to the name server.

Port [port_number]
Displays all events related to the port given by [port_number].

SNMP
Displays all events related to SNMP.

Switch
Displays all events related to switch management.

Zoning
Displays all events related to zoning.

level
Displays the event severity level logging setting and the display level setting.

options
Displays the options that are available for configuring event logging and automatic display to the screen. Refer to the for information about how to configure event logging and display level.

port
Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings
Displays the current filter settings for component, severity level, port, and display level. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples

The following is an example of the Show Log Component command:

```
SANbox2 #> show log component
Current settings for log
   ------------------------
   FilterComponent   NameServer MgmtServer Zoning Switch Blade Port Eport Snmp
```

The following is an example of the Show Log Level command:

```
SANbox2 #> show log level
   Current settings for log
   ------------------------
   FilterLevel       Info
   DisplayLevel      Critical
```

The following is an example of the Show Log Options command:

```
SANbox2 #> show log options
  Allowed options for log
  -----------------------
   FilterComponent
All,None,NameServer,MgmtServer,Zoning,Switch,Blade,Port,Eport,Snmp
   FilterLevel       Critical,Warn,Info,None
   DisplayLevel      Critical,Warn,Info,None
```

The following is an example of the Show Log command:

```
  SANbox2 #> show log
   [327][day month date time year][I][Eport Port:0/8][Eport State=
   E_A0_GET_DOMAIN_ID]
   [328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
   [329][day month date time year][I][Eport Port: 0/8][Sending init hello]
   [330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
   [331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
   [332][day month date time year][I][Eport Port: 0/8][EFP,WWN= 0x100000c0dd00b845,
   len= 0x30]
   [333][day month date time year][I][Eport Port: 0/8][Sending LSU oxid=0xc:type=1]
   [334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
   [335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
   [336][day month date time year][I][Eport Port: 0/8][Setting attribute
   Oper.UserPort.0.8.EpConnState Connected]
```

Show Perf Command

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second.

Authority None

Syntax

show perf
- byte
- inbyte
- outbyte
- frame
- inframe
- outframe
- errors

Keywords

byte
Displays continuous performance data in total bytes/second transmitted and received for all ports. Type “q” and press the Enter key to stop the display.

inbyte
Displays continuous performance data in bytes/second received for all ports. Type “q” and press the Enter key to stop the display.

outbyte
Displays continuous performance data in bytes/second transmitted for all ports. Type “q” and press the Enter key to stop the display.

frame
Displays continuous performance data in total frames/second transmitted and received for all ports. Type “q” and press the Enter key to stop the display.

inframe
Displays continuous performance data in frames/second received for all ports. Type “q” and press the Enter key to stop the display.

outframe
Displays continuous performance data in frames/second transmitted for all ports. Type “q” and press the Enter key to stop the display.

errors
Displays continuous error counts for all ports. Type “q” and press the Enter key to stop the display.

Examples

The following is an example of the Show Perf command:

```
SANbox2 #> show perf
Port   Bytes/s    Bytes/s    Bytes/s    Frames/s   Frames/s   Frames/s
  Number   (in)       (out)    (total)      (in)       (out)    (total)
  ------ -------    -------    -------    --------   --------   --------
  0      7K         136M       136M       245        68K        68K
  1      58K        0          58K        1K         0          1K
  2      0          0          0          0          0          0
  3      0          0          0          0          0          0
  4      0          0          0          0          0          0
  5      0          0          0          0          0          0
  6      0          7K         7K         0          245        245
  7      136M       58K        136M       68K        1K         70K
```

The following is an example of the Show Perf Byte command:

```
SANbox2 $> show perf byte
Displaying bytes/sec data...  (Press any key to stop display)

  0    1    2    3    4    5    6    7
  ------------------------------------------------------------------------------
  76M  0    0    32M  0    0    0    43M
  78M  0    0    34M  0    0    0    43M
  78M  0    0    34M  0    0    0    43M
  77M  0    0    33M  0    0    0    44M
  77M  0    0    33M  0    0    0    44M
  84M  0    0    40M  0    0    0    43M
  83M  0    0    39M  0    0    0    43M
  80M  0    0    35M  0    0    0    45M
  77M  0    0    33M  0    0    0    44M
  78M  0    0    33M  0    0    0    44M
  75M  0    0    29M  0    0    0    45M
  74M  0    0    28M  0    0    0    46M
q
```

Show Setup Command

Displays the current SNMP and system settings.

Authority None

Syntax **show setup**
- mfg
- radius
- services
- snmp
- system

Keywords **mfg**
Displays manufacturing information about the switch.

radius
Displays RADIUS server information.

services
Displays switch service status information.

snmp
Displays the current SNMP settings.

system
Displays the current system settings.

Examples The following is an example of the Show Setup Mfg command:

```
SANbox2 #> show setup mfg
  Manufacturing Information
  -------------------------
  BrandName                QLogic Corporation
  BuildDate                Unknown
  ChassisPartNumber        Unknown
  ChassisSerialNumber      S02300003
  CPUBoardSerialNumber     000603949
  MACAddress               00:c0:dd:00:90:aa
  PlanarPartNumber         Unknown
  SwitchSymbolicName       SANbox2
  SwitchWWN                10:00:00:c0:dd:00:90:ab
  SystemDescription        SANbox2-8c FC Switch
  SystemObjectID           1.3.6.1.4.1.1663.1.1.1.1.14
```

The following is an example of the Show Setup Services command:

```
SANbox2 #> show setup services
System Services
----------------------------
TelnetEnabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLMgmtEnabled            False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
ManagementServerEnabled   True
```

The following is an example of the Show Setup RADIUS command:

```
SANbox2 #> show setup radius

  Radius Information
  ------------------
  DeviceAuthOrder   RadiusLocal
  UserAuthOrder     RadiusLocal
  TotalServers      1

  Server: 1

  ServerIPAddress   10.20.11.8
  ServerUDPPort     1812
  DeviceAuthServer  False
  UserAuthServer    True
  AccountingServer  False
  Timeout           2
  Retries           0
  SignPackets       False
  Secret            ********
```

The following is an example of the Show Setup Snmp command:

```
SANbox2 #> show setup snmp
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           SANbox2-8c FC Switch
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
  Trap5Enabled          False
  ObjectID              1.3.6.1.4.1.1663.1.1.1.1.14
  AuthFailureTrap       True
  ProxyEnabled          True
```

The following is an example of the Show Setup System command:

```
SANbox2 #> show setup system
  System Information
  ------------------
  Eth0NetworkDiscovery     Static
  Eth0NetworkAddress       10.20.11.32
  Eth0NetworkMask          255.255.252.0
  Eth0GatewayAddress       10.20.8.254
  AdminTimeout             30
  InactivityTimeout        0
  LocalLogEnabled          True
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
  NTPClientEnabled         True
  NTPServerAddress         51.68.85.102
  EmbeddedGUIEnabled       True
```

Shutdown Command

Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

Authority Admin session

Syntax **shutdown**

Notes Always use this command to perform an orderly shut down before removing power from the switch.

When the shutdown is complete, the Heartbeat LED is extinguished.

Test Command

Tests ports using internal (SerDes level), external (transceiver), and online loopback tests. Internal and external tests require that the port be placed in diagnostic mode. Refer to the "Set Command" on page B-58 for information about changing the port administrative state. While the test is running, the remaining ports on the switch remain fully operational.

Authority Admin session

Syntax **test**

port [port_number] [test_type]
cancel
status

Keywords **port [port_number] *[test_type]***

Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

internal
Tests the SerDes for all port speeds independent of the capabilities of the transceiver. This is the default. The port must be in diagnostics mode to perform this test.

external
Tests both the SerDes and transceiver for all port speeds that are supported by the transceiver. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the transceiver.

online
Tests communications between the port and its device node or device loop at the operating port speed. The port being tested must be online and connected to a remote device. The port passes if the test frame that was sent by the ASIC matches the frame that is received. This test does not disrupt communication on the port.

cancel
Cancels the online test in progress.

status
Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Examples To run an internal or external port test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   ```
   admin start
   ```

2. Place the port in Diagnostics mode, enter the following command (*x* = port number) and press the Enter key.

   ```
   set port x state diagnostics
   ```

3. Choose the type of port loopback test to run:

   - To run an internal loopback test, enter the following:

     ```
     test port x internal
     ```

   - To run an external loopback test, enter the following command. A loopback plug must be installed for this test to pass.

     ```
     test port x external
     ```

4. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload.

5. After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.

6. After the test is run, put the port back into online state by entering the following command (*x* = port number) and pressing the Enter key.

   ```
   set port x state online
   ```

7. To verify port is back online, enter the following command and press the Enter key. The contents of the AdminState field should display be “Online”.

   ```
   show port x
   ```

The online loopback (node-to-node) test requires that port be online and connected to a remote device. To run the online loopback test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   ```
   admin start
   ```

2. To run the online loopback test, enter the following command and press the Enter key.

   ```
   test port x online
   ```

3. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

   ```
   SANbox2 (admin) #> test port x online

   A list of attributes with formatting and current values will
   follow. Enter a new value or simply press the ENTER key to
   accept the default value. If you wish to terminate this
   process before reaching the end of the list press 'q' or 'Q'
   and the ENTER key to do so.

     TestLength    (decimal value, 1-4294967295)   [100    ]
     FrameSize     (decimal value, 36-2148)        [256    ]
     DataPattern   (32-bit hex value or 'Default') [Default]
     StopOnError   (True/False)                    [False  ]
     Do you want to start the test? (y/n) [n]
   ```

4. After all parameter values are defined, press the Y key to start the test. After the command executes, a message on the screen will appear detailing the test results.

Uptime Command

Displays the elapsed up time since the switch was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority None

Syntax **uptime**

Examples The following is an example of the Uptime command:

```
SANbox2 #> uptime

  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

User Command

Administers and displays user accounts.

Authority Admin account name and an Admin session. The Accounts and List keywords are available to all account names without an Admin session.

Syntax

user
accounts
add
delete [account_name]
edit
list

Keywords

accounts
Displays all user accounts that exist on the switch. This keyword is available to all account names without an Admin session.

add
Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- A switch can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 8–20 characters.
- Admin authority grants permission to use the Admin command to open an admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The switch will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]
Deletes the account name given by [account_name] from the switch.

edit
Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list
Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is available to all account names without an Admin session.

Notes Authority level or password changes that you make to an account that is currently logged in do not take effect until that account logs in again.

Examples

The following is an example of the User Accounts command:

```
SANbox2 (admin) #> user accounts

    Current list of user accounts
  ----------------------------
  images       (admin authority = False, never expires)
  admin        (admin authority = True , never expires)
  chuckca      (admin authority = False, expires in < 50 days)
  gregj        (admin authority = True , expires in < 100 days)
  fred         (admin authority = True , never expires)
```

The following is an example of the User Add command:

```
SANbox2 (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 chars)  : *******

please confirm account password: *******

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

The following is an example of the User Edit command:

```
SB211.192 (admin) #> user edit

      Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'user1' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
SANbox2 (admin) #> user del user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
SANbox2 (admin) #> user list

    User                          Ethernet Addr-Port    Logged in Since
    ----                          ------------------    ---------------
  admin@OB-session1             10.20.68.108-1031     day month date time year
  admin@OB-session2             10.20.68.108-1034     day month date time year
  snmp@OB-session3              Unknown               day month date time year
  snmp@IB-session4              Unknown               day month date time year
  admin@OB-session5             Unknown               day month date time year
```

Whoami Command

Displays the account name, session number, and switch domain ID for the Telnet session.

Authority None

Syntax **whoami**

Examples The following is an example of the Whoami command:

```
SANbox2 #> whoami

User name       : admin@session2
Switch name     : SANbox2
Switch domain ID: 21 (0x15)
```

Zone Command

Manages zones and zone membership on a switch.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page B-129 for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available without an Admin session.

Syntax

zone
add [zone] [member_list]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
members [zone]
remove [zone] [member_list]
rename [zone_old [zone_new]
type [zone] *[zone_type]*
zonesets [zone]

Keywords

add [zone] [member_list]
Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a member exists.

copy [zone_source] [zone_destination]
Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]
Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 2000 zones.

delete [zone]
Deletes the specified zone given by [zone] from the zoning database. If the zone is a component of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all zones and the zone sets of which they are components. This keyword does not require an Admin session.

members [zone]
Displays all members of the zone given by [zone]. This keyword does not require an Admin session.

remove [zone] [member_list]
Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

rename [zone_old] [zone_new]
Renames the zone given by [zone_old] to the zone given by [zone_new].

type [zone] ***[zone_type]***
Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone]. [zone_type] can be one of the following:

soft – name server zone

hardACL – Access control list hard zone. This keyword is case sensitive.

zonesets [zone]
Displays all zone sets of which the zone given by [zone] is a component. This keyword does not require an Admin session.

Examples The following is an example of the Zone List command:

```
SANbox2 #> zone list

  Zone        ZoneSet
  -------------------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_1

  wwn_2215c3
              zone_set_1

  wwn_0160ed
              zone_set_1

  wwn_c001b0
              zone_set_1

  wwn_401248
              zone_set_1

  wwn_02402f
              zone_set_1

  wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
SANbox2 #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
SANbox2 #> zone zonesets zone1

  Current List of ZoneSets for Zone: zone1
  ---------------------------------
  zone_set_1
```

Zoneset Command

Manages zone sets and component zones across the fabric.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page B-129 for information about starting a Zoning Edit session. The Active, List, and Zones keywords are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

zoneset
activate [zone_set]
active
add [zone_set] [zone_list]
copy [zone_set_source] [zone_set_destination]
create [zone_set]
deactivate
delete [zone_set]
list
remove [zone_set] [zone_list]
rename [zone_set_old] [zone_set_new]
zones [zone_set]

Keywords

activate [zone_set]
Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active
Displays the name of the active zone set. This keyword does not require Admin session.

add [zone_set] [zone_list]
Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list].

copy [zone_set_source] [zone_set_destination]
Creates a new zone set named [zone_set_destination] and copies into it the zones from the zone set given by [zone_set_source].

create [zone_set]
Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 zone sets.

deactivate
Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]
Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list
Displays a list of all zone sets. This keyword does not require an Admin session.

remove [zone_set] [zone_list]
Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated.

rename [zone_set_old] [zone_set_new]
Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set.

zones [zone_set]
Displays all zones that are components of the zone set given by [zone_set]. This keyword does not require an Admin session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a component of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
SANbox2 #> zoneset active

  ActiveZoneSet    Bets
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

The following is an example of the Zoneset List command:

```
SANbox2 #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

The following is an example of the Zoneset Zones command:

```
SANbox2 #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Zoning Command

Opens a Zoning Edit session in which to create and manage zone sets and zones. Refer to the "Zone Command" on page B-123 and the "Zoneset Command" on page B-127.

Authority Admin session except for the Active, History, Limits, and List keywords. The Clear keyword also requires a zoning edit session.

Syntax

zoning
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays information for the active zone set including component zones and zone members. This keyword does not require an Admin session.

cancel
Closes the current Zoning Edit session. Any unsaved changes are lost.

clear

Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword requires a zoning edit session. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

Note: The preferred method for clearing the zoning database from the switch is the Reset Zoning command.

edit
Opens a Zoning Edit session.

history
Displays a history of zoning modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits
Displays the number of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database. This keyword also displays the switch zoning database limits, excluding the active zone set, which are described in Table B-29. This keyword does not require an Admin session.

Table B-29. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256)
MaxZones	Maximum number of zones (2000)
MaxAliases	Maximum number of aliases (2500)
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch's zoning database.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2000), excluding those in the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

list
Lists all zoning definitions. This keyword does not require an Admin session.

restore
Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.

save
Saves changes made during the current Zoning Edit session. The system informs you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples

The following is an example of the Zoning Edit command:

```
SANbox2 #> admin start
SANbox2 (admin) #> zoning edit
SANbox2 (admin-zoning) #>
.
.
SANbox2 (admin-zoning) #> zoning cancel

  Zoning edit mode will be canceled.  Please confirm (y/n): [n]   y

SANbox2 (admin) #> admin end
```

The following is an example of the Zoning Limits command:

```
SANbox2 #> zoning limits

  Zoning Attribute     Maximum   Current   [Zoning Name]
  ----------------     -------   -------   -------------
  MaxZoneSets          256       6
  MaxZones             2000      17
  MaxAliases           2500      1
  MaxTotalMembers      10000     166f
  MaxZonesInZoneSets   2000      19
  MaxMembersPerZone    2000
                                 10        D_1_JBOD_1
                                 23        D_1_Photons
                                 9         D_2_JBOD1
                                 16        D_2_NewJBOD_2
                                 5         E1JBOD1
                                 5         E2JBOD2
                                 3         LinkResetZone
                                 3         LinkResetZone2
                                 8         NewJBOD1
                                 8         NewJBOD2
                                 24        Q_1Photon1
                                 8         Q_1_NewJBOD1
                                 13        Q_1_Photon_1
                                 21        Q_2_NewJBOD2
                                 3         ZoneAlias
                                 3         ZoneDomainPort
                                 4         ZoneFCAddr
  MaxMembersPerAlias   2000
                                 2         AliasInAZone
```

The following is an example of the Zoning List command:

```
SANbox2 #> zoning list
  Active ZoneSet Information
  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3
  Configured Zoning Information
  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:
```

Glossary

Access Control List Zone

Access Control List zoning divides the fabric for purposes of controlling discovery and inbound traffic.

Active Zone Set

The zone set that defines the current zoning for the fabric.

Active Firmware

The firmware image on the switch that is in use.

Activity LED

A port LED that indicates when frames are entering or leaving the port.

Administrative State

State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm

A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

Alias

A named set of ports or devices. An alias is not a zone, and can not have a zone or another alias as a member.

AL_PA

Arbitrated Loop Physical Address

Arbitrated Loop

A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA)

A unique one-byte value assigned during loop initialization to each NL_Port on a loop.

ASIC

Application Specific Integrated Circuit

Auto Save

Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch.

BootP

A type of network server.

Buffer Credit

A measure of port buffer capacity equal to one frame.

Cascade Topology

A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.

Class 2 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Class 3 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Configured Zone Sets

The zone sets stored on a switch excluding the active zone set.

Default Visibility

Zoning parameter that determines the level of communication among ports/devices when there is no active zone set.

Domain ID

User defined number that identifies the switch in the fabric.

Event Log

Log of messages describing events that occur in the fabric.

Expansion Port

E_Port that connects to another FC-SW-2 compliant switch.

Fabric Database

The set of fabrics that have been opened during a SANsurfer Switch Manager session.

Fabric Device Management Interface

An interface by which device host bus adapters can be managed through the fabric.

Fabric Management Switch

The switch through which the fabric is managed.

Fabric Name

User defined name associated with the file that contains user list data for the fabric.

Fabric Port

An F_Port or FL_Port.

Fabric Security

The functions that provide security for fabric users and devices including user account security and fabric services.

Fabric Services

A component of fabric security that provides for the control of inband management and SNMP on a switch.

Fabric View File

A file containing a set of fabrics that were opened and saved during a previous SANsurfer Switch Manager session.

Fan Fail LED

An LED that indicates that a cooling fan in the switch is operating below standard.

FDMI

See Fabric Device Management Interface.

Flash Memory

Memory on the switch that contains the chassis control firmware.

Force PROM Mode

See Maintenance Mode.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU

Field Replaceable Unit

Heartbeat LED

A chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

Inactive Firmware

The firmware image on the switch that is not in use.

Inband Management

The ability to manage a switch through another switch over an inter-switch link.

Initiator

The device that initiates a data exchange with a target device.

In-Order-Delivery

A feature that requires that frames be received in the same order in which they were sent.

Input Power LED

A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Inter-Switch Link

The connection between two switches using E_Ports.

IP

Internet Protocol

LIP

Loop Initialization Primitive sequence

Logged-In LED

A port LED on SANbox2-8c and SANbox2-16 switches that indicates device login or loop initialization status.

Maintenance Button

Formerly known as the Force PROM button. Momentary button on the switch used to reset the switch or place the switch in maintenance mode.

Maintenance Mode

Formerly known as force PROM mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.

Management Information Base

A set of guidelines and definitions for SNMP functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

Mesh Topology

A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB

Management Information Base

Multistage Topology

A fabric in which two or more edge switches connect to one or more core switches.

Network Time Protocol

A network protocol that enables a client to synchronize its time with a server.

NL_Port

Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

NTP

Network Time Protocol

Over Temperature LED

A chassis LED or a power supply LED that indicates that the switch or power supply is overheating.

Pending Firmware

The firmware image that will be activated upon the next switch reset.

POST

Power On Self Test

Power On Self Test (POST)

Diagnostics that the switch chassis performs at start up.

Principal Switch

The switch in the fabric that manages domain ID assignments.

SANsurfer Switch Manager

Switch management application.

SFP

Small Form-Factor Pluggable.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SNMP

Simple Network Management Protocol

Soft Zone

Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone.

Target

A storage device that responds to an initiator device.

User Account

An object stored on a switch that consists of an account name, password, authority level, and expiration date.

User Account Security

A component of fabric security that provides for the administration and authentication of account names, passwords, expiration dates, and authority level.

VCCI

Voluntary Control Council for Interference

Worldwide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

Worldwide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database

The set of zone sets, zones, and aliases stored on a switch.

Notes

Index

D

E

F

G

H

I

R

S

T

Notes